著作権保護システム

著作権保護システム、鍵生成装置、記録装置、再生装置、読み出し装置、復号装置、記録媒体、記録方法、再生方法、及びプログラム

技術分野

本発明は、映画や音楽などの著作物をデジタル化したコンテンツを、光ディスク等の大容量記録媒体に記録して、再生するシステムに関し、特にコンテンツの著作者の許可なく不正利用されることを防止する著作権保護システムに関する。

背景技術

近年、記録媒体が大容量化するに従い、映画や音楽などの著作物をデジタル化したコンテンツを例えば光ディスク等の記録媒体に格納して市販するビジネスが盛んに行われている。

記録媒体に記録されたコンテンツは、不正にコピーされる可能性があるため、何らかの保護が必要である。

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピー等といった不正利用を防止するために暗号化技術が用いられる。

具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号し、コンテンツの再生等を行うことができる。

なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化

して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法とがある。

このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析によって、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する再生装置あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを実現する技術を鍵無効化技術と呼び、鍵無効化を実現するシステムとして、特許文献１（特開２００２－２８１０１３号公報）が開示されている。

一方、記録媒体に記録された暗号化コンテンツを再生する装置としては、記録媒体から暗号化コンテンツを読み出す機能と読み出した暗号化コンテンツを復号する機能が一体となったいわゆる民生用プレーヤや、パソコンに接続もしくは内蔵された光ディスクドライブで記録媒体から暗号化コンテンツを読み出し、読み出した暗号化コンテンツをパソコンのホスト上で動作するアプリケーションプログラムによって復号して再生するものがある。これら２つの種類の再生装置に対応する著作権保護システムとして、非特許文献１（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｐｒｅｒｅｃｏｒｄｅｄ　Ｍｅｄｉａ　ＤＶＤ　Ｂｏｏｋ、４Ｃ　Ｅｎｔｉｔｙ，ＬＬＣ）が公開されている。

しかしながら、上記したような従来の著作権保護システムでは、対象とするすべての種類の再生装置に対して共通の無効化データを記録媒体に記録するようにしているため、各再生装置はその無効化データ全体を記録媒体から読み込んで少なくとも一時的に格納するメモリを装置内に

設ける必要がある。

また、一般にＤＶＤプレーヤ等の民生用プレーヤにおいては、装置に組み込まれた処理アルゴリズムや鍵の長さを変更することは、時間と手間がかかり困難である。

一方、パソコン上のアプリケーションプログラムとして復号処理や鍵がソフトウェアで実装される場合は、一般的にハードウェアで実装する場合に比べて、内蔵する復号アルゴリズムや鍵の更新や追加は容易であるが、復号アルゴリズムや鍵の堅牢な実装は困難である。しかしながら、従来の共通の無効化データを記録媒体に記録する著作権保護システムでは、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露された場合であっても、暗号化・復号のアルゴリズムや鍵長を変更することは実質上不可能となっている。これは、無効化機能が正しく働かなくなることを意味し、不正機器によりコンテンツの不正利用が蔓延することにつながる。また、パソコンで使用されるアプリケーションの鍵やアルゴリズムが一旦暴露された場合においては、これが民生機器に及んで全ての機器において適切に無効化機能が働かなくなるような場合も考えられる。

本発明では、上記課題を解決するために、再生装置内に設けるメモリのサイズを小さくでき、かつ、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露された場合でも、暗号化・復号のアルゴリズムや鍵長を変更することでシステム全体の無効化機能を維持することのできる著作権保護システムを提供する。

発明の開示

本発明は、コンテンツを暗号化して記録する記録装置と、前記暗号化

コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記記録装置は、メディア鍵と前記Ｎ個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化し、前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであぅて、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、前記各カテゴリの再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵を生成し、少なくとも前記Ｎ個の暗号化メディア鍵データと前記Ｎ個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録し、前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、前記著作権システムであって、前記再生装置は、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第２のカテゴリに属する第２再生装置、及び前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第２のカテ

ゴリの読み出し装置と前記第２のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第１のカテゴリの復号装置とから構成される第１再生装置とから成り、前記記録装置は、メディア鍵と前記第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、少なくとも前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、前記第２再生装置は、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号し、前記第１再生装置において、前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記第１の無効化データを前記第１カテゴリの復号装置に供給し、前記第１のカテゴリの復号装置は、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施し前記コンテンツを取得することを特徴とする。

また、本発明は、コンテンツを暗号化して記録する記録装置であって、前記記録装置は、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化

するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

また、本発明は、前記記録装置であって、前記Ｎ個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。

また、前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化することを特徴とする。

また、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録することを特徴とする。

また、本発明は、前記記録装置であって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵データを生成し、少なくとも前記Ｎ個の暗号化メディア鍵データと前記Ｎ個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録することを特徴とする。

また、前記記録装置は、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効

化するための第２の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、少なくとも前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

また、本発明は、暗号化コンテンツが記録される記録媒体であって、前記記録媒体には、少なくとも、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツが記録されることを特徴とする。

また、本発明は、前記記録媒体であって、前記Ｎ個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。

また、本発明は、前記記録媒体であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであることを特徴とする。

また、本発明は、前記記録媒体であって、前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されることを特徴とする。

また、本発明は、前記記録媒体であって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記コンテンツ鍵を

前記Ｎ個のメディア鍵で暗号化して生成されたＮ個の暗号化コンテンツ鍵が記録されることを特徴とする。

また、前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとが記録されることを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記記録媒体には、少なくともメディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵デー

タを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであり、

前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記N個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記コンテンツ鍵を前記N個のメディア鍵で暗号化して生成されたN個の暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コ

ンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、再生装置であって、前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記第２のカテゴリに属し、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記読み出し装置は、前記第２のカテゴリに属し、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第

１の無効化データを出力することを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第１の無効化データを出力し、前記復号装置は、前記第１のカテゴリに属し、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施して前記コンテンツを取得することを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、請求項２５記載の読み取り装置と請求項２６記載の復号装置とから構成されることを特徴とする。

また、本発明は、コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前

記記録装置及び前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録し、前記記録装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

また、本発明は、鍵生成装置であって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録することを特徴とする。

また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録

媒体から、前記Ｎ個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

また、本発明は、コンテンツを暗号化して記録する記録装置に用いる記録方法であって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成する生成ステップと、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成する暗号化コンテンツ生成ステップと、少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する記録ステップとを含むことを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置に用いる再生方法であって、前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記記録媒体には、少なくともメディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記再生方法は、前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み出しステップと、前記読み出しステップにおいて読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する復号ステップとを含むことを特徴とする。

また、本発明は、コンテンツを暗号化して記録する記録装置に用いる

プログラムであって、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成する生成ステップと、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成する暗号化コンテンツ生成ステップと、少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する記録ステップとを含むことを特徴とする。

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置に用いるプログラムであって、前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、前記記録媒体には、少なくともメディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記プログラムは、前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み出しステップと、前記読み出しステップにおいて読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する復号ステップとを含むことを特徴とする。

図面の簡単な説明

図１は、本発明の実施の形態１における記録装置及び記録媒体を示すブロック図である。

図２は、本発明の実施の形態１における記録媒体及び第１のカテゴリの再生装置を示すブロック図である。

図３は、本発明の実施の形態１における記録媒体及び第２のカテゴリの再生装置を示すブロック図である。

図４は、本発明の実施の形態１における記録媒体に記録するデータの具体例を示す模式図である。

図５は、本発明の実施の形態１におけるシステム更新の具体例１を示す模式図である。

図６は、本発明の実施の形態１におけるシステム更新の具体例２を示す模式図である。

図７は、本発明の実施の形態２における鍵生成装置及び記録媒体を示すブロック図である。

図８は、本発明の実施の形態２における第１のカテゴリの記録装置及び記録媒体を示すブロック図である。

図９は、本発明の実施の形態２における第２のカテゴリの記録装置及び記録媒体を示すブロック図である。

図１０は、本発明の実施の形態２における記録媒体及び第１のカテゴリの再生装置を示すブロック図である。

図１１は、本発明の実施の形態２における記録媒体及び第２のカテゴリの再生装置を示すブロック図である。

図１２は、本発明の実施の形態２における記録媒体に記録するデータの具体例を示す模式図である。

図１３は、本発明の実施の形態３における記録装置及び記録媒体を示すブロック図である。

図１４は、本発明の実施の形態３における記録媒体及び第１のカテゴリの再生装置を示すブロック図である。

図１５は、本発明の実施の形態３における記録媒体及び第２の再生装置を示すブロック図である。

図１６は、本発明の実施の形態３における記録媒体に記録するデータの具体例を示す模式図である。

図１７は、本発明の実施の形態３におけるシステム更新の具体例１を示す模式図である。

図１８は、本発明の実施の形態３におけるシステム更新の具体例２を示す模式図である。

図１９は、本発明の実施の形態４における記録装置及び記録媒体を示すブロック図である。

図２０は、本発明の実施の形態４における記録媒体及び第１の再生装置を示すブロック図である。

図２１は、本発明の実施の形態４における記録媒体及び第２の再生装置を示すブロック図である。

図２２は、本発明の実施の形態４における記録媒体に記録するデータの具体例を示す模式図である。

図２３は、本発明の実施の形態４におけるシステム更新の具体例１を示す模式図である。

図２４は、本発明の実施の形態４におけるシステム更新の具体例２を示す模式図である。

図２５は、本発明の実施の形態５における記録装置及び記録媒体を示すブロック図である。

図２６は、本発明の実施の形態５における記録媒体及び第１の再生装置を示すブロック図である。

図２７は、本発明の実施の形態５における記録媒体及び第２の再生装置を示すブロック図である。

図２８は、本発明の実施の形態５における記録媒体に記録するデータの具体例を示す模式図である。

図２９は、本発明の実施の形態５におけるシステム更新の具体例１を示す模式図である。

図３０は、本発明の実施の形態５におけるシステム更新の具体例２を示す模式図である。

図３１は、本発明の実施の形態６における記録装置及び記録媒体を示すブロック図である。

図３２は、本発明の実施の形態６における記録媒体及び第１の再生装置を示すブロック図である。

図３３は、本発明の実施の形態６における記録媒体及び第２の再生装置を示すブロック図である。

図３４は、本発明の実施の形態６における記録媒体に記録するデータの具体例を示す模式図である。

図３５は、本発明の実施の形態６におけるシステム更新の具体例１を示す模式図である。

図３６は、本発明の実施の形態６におけるシステム更新の具体例２を示す模式図である。

図３７は、本発明の実施の形態７における記録装置及び記録媒体を示すブロック図である。

図３８は、本発明の実施の形態７における記録媒体及び第１の再生装置を示すブロック図である。

図３９は、本発明の実施の形態７における記録媒体及び第２の再生装置を示すブロック図である。

図４０は、本発明の実施の形態７における記録媒体に記録するデータの具体例を示す模式図である。

図４１は、本発明の実施の形態７におけるシステム更新の具体例１を示す模式図である。

図４２は、本発明の実施の形態７におけるシステム更新の具体例２を示す模式図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を参照しながら説明する。

（実施の形態１）

本発明の実施の形態１は、再生専用のＤＶＤ等の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。尚、本実施の形態１においては、再生装置側に第１及び第２のカテゴリを設けて、カテゴリ毎に異なるデバイス鍵を用いて無効化を行う。このため、同一の記録媒体に用いる無効化システムを再生装置側のカテゴリにより分類でき、たとえ一方の無効化システムが破られた場合においても、他のカテゴリに属する無効化システムは維持できることを特徴とする。

以下、本発明の実施の形態１について、図面を参照しながら説明する。図１は、コンテンツを暗号化して記録する記録装置１００及び記録媒体１２０を示しており、図２は、記録媒体１２０から暗号化コンテンツを読み出して復号する第１のカテゴリの再生装置２００を示しており、図３は、記録媒体１２０から暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置３００を示している。また、図４は記録媒体１２０に記録される各種データの具体例を示している。

記録装置１００は、例えば、製造時において各ＤＶＤにコンテンツを記録するような装置であり、第１のカテゴリの各再生装置が秘密に保有するデバイス鍵を格納する第１のデバイス鍵格納部１０１と、第２のカテゴリの各再生装置が秘密に保有するデバイス鍵を格納する第２のデバイス鍵格納部１０２と、メディア鍵を暗号化するために用いるデバイス

鍵を選択する第１のデバイス鍵選択部１０３及び第２のデバイス鍵選択部１０４と、外部から入力されるメディア鍵を第１のデバイス鍵選択部１０３で選択したデバイス鍵で暗号化する第１のメディア鍵暗号化部１０５と、メディア鍵を第２のデバイス鍵選択部１０４で選択したデバイス鍵で暗号化する第２のメディア鍵暗号化部１０６と、外部から入力されるコンテンツ鍵をメディア鍵で暗号化するコンテンツ鍵暗号化部１０７と、同じく外部から入力されるコンテンツを暗号化するコンテンツ暗号化部１０８とを備える。

なお、図１には示していないが、第１のメディア鍵暗号化部１０５には、第１のカテゴリの再生装置のうち無効化すべき再生装置の情報が、第２のメディア鍵暗号化部１０６には第２のカテゴリの再生装置のうち無効化すべき再生装置の情報が、それぞれ入力されており、暗号化メディア鍵を生成する際にこれら無効化すべき再生装置では正しいメディア鍵が復号できないように暗号化メディア鍵を生成する。さらにメディア鍵は記録媒体を製造する度に、コンテンツ鍵はコンテンツ毎に異なる鍵データを選択している。

記録媒体１２０は、第１のメディア鍵暗号化部１０５が生成した第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域１２１と、第２のメディア鍵暗号化部１０６が生成した第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域１２２と、コンテンツ鍵暗号化部１０７が生成した暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域１２３と、コンテンツ暗号化部１０８が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域１２４とを備える。

第１のカテゴリの再生装置２００は、デバイス鍵を秘密に保有するデバイス鍵格納部２０１と、デバイス鍵を用いて記録媒体１２０から読み

出した第１の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部２０２と、取得したメディア鍵を用いて記録媒体１２０から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部２０３と、取得したコンテンツ鍵を用いて記録媒体１２０から読み出した暗号化コンテンツを復号するコンテンツ復号部２０４とを備える。本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される再生装置を第１のカテゴリに属する再生装置とした。

第２のカテゴリの再生装置３００は、デバイス鍵を秘密に保有するデバイス鍵格納部３０１と、デバイス鍵を用いて記録媒体１２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部３０２と、取得したメディア鍵を用いて記録媒体１２０から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部３０３と、取得したコンテンツ鍵を用いて記録媒体１２０から読み出した暗号化コンテンツを復号するコンテンツ復号部３０４とを備える。本実施の形態では一般的な民生プレーヤのようにハードウェアで実装される再生装置を第２のカテゴリに属する再生装置とした。

図４は、ｍ台の第１のカテゴリの再生装置及びｎ台の第２のカテゴリの再生装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの再生装置２と第２のカテゴリの再生装置３が無効化されているとした場合の、記録媒体１２０に記録される各種データの具体例を示している。図４中で、第１のカテゴリの再生装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの再生装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＢｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）及びＥｄ（Ｘ，Ｙ）はデータＹ

を鍵データＸを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長５６ｂｉｔのＤＥＳ暗号を使用した。

（第１の暗号化メディア鍵データ記録領域１２１）

第１の暗号化メディア鍵データ記録領域１２１には、第１のカテゴリの再生装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化されたメディア鍵（ＭＫ）が記録されている。ここで、第１のカテゴリの再生装置２は無効化されており、ＤＫＡ２ではメディア鍵（ＭＫ）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第１の暗号化メディア鍵を生成する際に、第１のメディア鍵暗号化部１０５において、第１のカテゴリのうち無効化すべき再生装置の情報として再生装置２が入力され、再生装置２では正しいメディア鍵が得られないように処理された結果である。

（第２の暗号化メディア鍵データ記録領域１２２）

第２の暗号化メディア鍵データ記録領域１２２には、第２のカテゴリの再生装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｎ）で暗号化されたメディア鍵（ＭＫ）が記録されている。ここで、第２のカテゴリの再生装置３は無効化されており、ＤＫＢ３ではメディア鍵（ＭＫ）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第２の暗号化メディア鍵を生成する際に、第２のメディア鍵暗号化部１０６において、第２のカテゴリのうち無効化すべき再生装置の情報として再生装置３が入力され、再生装置３では正しいメディア鍵が得られないように処理された結果である。

第１及び第２の暗号化メディア鍵データをこのように生成することにより、第１のカテゴリの再生装置２及び第２のカテゴリの再生装置３を除く再生装置が正しいメディア鍵（ＭＫ）を復号することができるとと

もに、第１のカテゴリの再生装置２及び第２のカテゴリの再生装置３をシステムから排除することができる。

（暗号化コンテンツ鍵記録領域１２３）

暗号化コンテンツ鍵記録領域１２３にはメディア鍵（ＭＫ）で暗号化されたコンテンツ鍵（ＣＫ）が記録されている。

（暗号化コンテンツ記録領域１２４）

暗号化コンテンツ記録領域１２４には、コンテンツ鍵（ＣＫ）で暗号化されたコンテンツが記録されている。

以上のように構成された本発明の実施の形態１において、例えば第１のカテゴリの再生装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの再生装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの再生装置の無効化システムを更新することになる。以下、その具体例を説明する。

（システム更新の具体例１）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成される記録媒体１２０に記録する各種データの具体例１を図５に示す。図４との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ)のどれとも一致しないようになっている。このため、無効化が機能しなくなった以後の記録媒体１２０の製造時において無効化システムを更新することが可能となる。

一方、無効化されていない第１のカテゴリの再生装置２００には、新たなデバイス鍵が付与され、デバイス鍵格納部２０１に格納される。例

えば、第１のカテゴリの再生装置ｍは、以前から保有していたデバイス鍵（ＤＫＡｍ）に加え、新たに付与されたデバイス鍵（ＤＫＡ’ｍ）をデバイス鍵格納部２０１に保有する。再生装置ｍは、図４の記録媒体を再生する際には、デバイス鍵ＤＫＡｍを用い、無効化システム更新後の図５の記録媒体を再生する際には、デバイス鍵ＤＫＡ’ｍを用いて、記録媒体から読み出した第１の暗号化メディア鍵を復号してメディア鍵（ＭＫ）を取得し、取得したメディア鍵（ＭＫ）を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号再生する。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図５の記録媒体から読み出した第１の暗号化メディア鍵を復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。

（システム更新の具体例２）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成される記録媒体１２０に記録する各種データの具体例２を図６に示す。図４との違いは、第１の暗号化メディア鍵の生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことと、暗号化アルゴリズムをＥａ（Ｘ；Ｙ）からＥａ’（Ｘ，

Y）に変更したことである。ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっている。

一方、無効化されていない第１のカテゴリの各再生装置２００には、新たなデバイス鍵を付与されデバイス鍵格納部２０１に格納される。また、メディア鍵復号部２０２には、以前から組み込まれている図４の第１の暗号化メディア鍵データを復号するための復号アルゴリズムＤａ（Ｘ，Ｙ）に加えて、図５の第１の暗号化メディア鍵データを復号するための復号アルゴリズムＤａ’（Ｘ，Ｙ）が組み込まれる。例えば、第１のカテゴリの再生装置ｍは、以前から保有していたデバイス鍵（ＤＫＡｍ）に加え、新たに付与されたデバイス鍵（ＤＫＡ’ｍ）を保有する。再生装置ｍは、図４の記録媒体を再生する際には、デバイス鍵ＤＫＡｍと暗号化アルゴリズムＤａ（Ｘ，Ｙ）を用い、図５の記録媒体を再生する際には、デバイス鍵ＤＫＡ’ｍと暗号アルゴリズムＤａ’（Ｘ，Ｙ）を用いて、記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得し、取得したメディア鍵（ＭＫ）を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号する。本実施の形態ではＥａ（Ｘ，Ｙ）及びＤａ（Ｘ，Ｙ）は鍵長５６ｂｉｔのＤＥＳ暗号を用いたのに対して、Ｅａ’（Ｘ，Ｙ）及びＤａ’（Ｘ，Ｙ）では２キートリプルＤＥＳと呼ばれる鍵長１１２ｂｉｔの暗号を用いた。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図５の記録媒体から読み出した第１の暗号化メ

ディア鍵データを復号してメディア鍵(ＭＫ)を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）及び第２の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。

なお、システム更新の具体例１、２ともに記録媒体にはシステム更新の世代に関する情報を記録しており、第１のカテゴリの再生装置はこの情報に基づいて、いずれの世代のデバイス鍵あるいはアルゴリズムを使用するかを判断する。

以上のように構成された本発明の実施の形態１によれば、第１のカテゴリの再生装置２００及び第２のカテゴリの再生装置３００は、それぞれ異なるカテゴリの再生装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの再生装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの再生装置に影響を与えることなく、無効化システムを変更することが可能になる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易では

あるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。そして、例えば、第１カテゴリに属する再生装置は、アプリケーションでコンテンツの復号を実現するＰＣ、第２カテゴリに属する再生装置としては、ハードウェアでコンテンツの復号を実現するＤＶＤプレーヤ等の民生機器が挙げられる。

なお、本実施の形態では図１において、メディア鍵及びコンテンツ鍵が記録装置１００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置１００がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置１００がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

また、本実施の形態では図１において、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵をメディア鍵で暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する１階層の構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図１に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図１中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置さ

れる装置に内蔵され、コンテンツ暗号化部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図５のＥａ（ＤＫＡ’２，０）や図６のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する再生装置の台数を増やすことが可能となる。

また、本実施の形態では、図４に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

（実施の形態２）

本発明の実施の形態２は、書き換え型もしくは追記型のＤＶＤ－ＲＡＭやＤＶＤ－Ｒ等の記録媒体にＤＶＤレコーダ等の記録装置でコンテンツ鍵を用いて暗号化したコンテンツを記録し、再生装置で暗号化コンテンツをコンテンツ鍵で復号化した後に再生するシステムに本発明を適用することを特徴としている。

以下、本発明の実施の形態２について、図面を参照しながら説明する。図７は、鍵情報を生成して記録する鍵生成装置７００及び記録媒体７２０を示しており、図８は、記録媒体７２０にコンテンツを暗号化して記録する第１のカテゴリの記録装置８００を示しており、図９は、記録媒体７２０にコンテンツを暗号化して記録する第２のカテゴリの記録装置９００を示しており、図１０は記録媒体７２０から暗号化コンテンツを読み出して復号する第１のカテゴリの再生装置１０００を示しており、図１１は記録媒体７２０から暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置１１００を示している。また、図１２は、記録媒体７２０に記録される各種データの具体例を示している。

鍵生成装置７００は、第１のデバイス鍵格納部７０１に第１のカテゴリの各装置が秘密に保有するデバイス鍵を、第２のデバイス鍵格納部７０２に第２のカテゴリの各装置が秘密に保有するデバイス鍵を、それぞれ格納する。メディア鍵及びコンテンツ鍵の暗号化については、前記した実施の形態１における記録装置と同様であるので、その説明は省略する。

記録媒体７２０は、第１の暗号化メディア鍵データ記録領域７２１と、第２の暗号化メディア鍵データ記録領域７２２と、暗号化コンテンツ鍵記録領域７２３と、暗号化コンテンツ記録領７２４とを備える。ここで、破線で囲んだ、第１の暗号化メディア鍵データ記録領域７２１、第２の

暗号化メディア鍵データ記録領域７２２、及び、暗号化コンテンツ鍵記録領域７２３は、第１のカテゴリの記録装置８００及び第２のカテゴリの記録装置９００では記録不可能な領域である。一方、暗号化コンテンツ記録領域は、第１のカテゴリの記録装置８００及び第２のカテゴリの記録装置９００で記録可能な領域である。

第１のカテゴリの記録装置８００は、デバイス鍵を秘密に保有するデバイス鍵格納部８０１と、デバイス鍵を用いて記録媒体７２０から読み出した第１の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部８０２と、取得したメディア鍵を用いて記録媒体から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部８０３と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部８０４とを備える。本実施の形態では、パソコン上のアプリケーションプログラムのようにソフトウェアで実装される記録装置を第１のカテゴリに属する記録装置とした。

第２のカテゴリの記録装置９００は、デバイス鍵を秘密に保有するデバイス鍵格納部９０１と、デバイス鍵を用いて記録媒体７２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部９０２と、取得したメディア鍵を用いて記録媒体から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部９０３と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部９０４とを備える。本実施の形態では、一般的な民生レコーダのようにハードウェアで実装される記録装置を第２のカテゴリに属する記録装置とした。

第１のカテゴリの再生装置１０００及び第２のカテゴリの再生装置１１００は、それぞれ前記した本発明の実施の形態１における第１のカテ

ゴリの再生装置２００及び第２のカテゴリの再生装置３００と同じ構成であり、同一の構成要素には同一の符号を付し、その説明を省略する。

図１２は、ｍ台の第１のカテゴリの装置、及びｎ台の第２のカテゴリの装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの装置２と第２のカテゴリの装置３が無効化されているとした場合の、記録媒体７２０に記録される各種データの具体例を示している。図１２中で、第１のカテゴリの装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＢｊとしている。なお、第１の暗号化メディア鍵データ記録領域７２１、第２の暗号化メディア鍵データ記録領域７２２、暗号化コンテンツ鍵データ記録領域７２３、及び暗号化コンテンツ記録領域７２４に記録されるデータは、それぞれ前記した本発明の実施の形態１における第１の暗号化メディア鍵データ記録領域１２１、第２の暗号化メディア鍵データ記録領域１２２、暗号化コンテンツ鍵データ記録領域１２３、及び暗号化コンテンツ記録領域１２４に記録されるデータと同じであるので、その説明を省略する。

本実施の形態によれば、上記した構成により、第１のカテゴリの装置２及び第２のカテゴリの装置３を除く装置が正しいメディア鍵（ＭＫ）を復号することができるとともに、第１のカテゴリの装置２及び第２のカテゴリの装置３をシステムから排除することができる。

また、本実施の形態において、第１のカテゴリの装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの装置の無効化システムを更新することになる。更新の方法については、前記した本発明の実施の形態１の場合と同様の方法がとれるので、その説明を省略する。

なお、システムの更新に際して、第２の暗号化メディア鍵の生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２

のカテゴリに属する記録装置及び再生装置には何らの変更を加える必要がない。

以上のように構成された本発明の実施の形態２によれば、第１のカテゴリの装置（記録装置８００及び再生装置１０００）及び第２のカテゴリの装置（記録装置９００及び再生装置１１００）は、それぞれ異なるカテゴリの装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される装置とした場合に、特に有効である。

なお、本実施の形態では、各カテゴリの記録装置と再生装置が別々の装置である形態としたが、本発明はそれに限定されるものではない。例えば、記録装置と再生装置が同一の装置である形態であっても良い。

また、本実施の形態では図７において、メディア鍵及びコンテンツ鍵が鍵生成装置７００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、鍵生成装置７００がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。ま

た、鍵生成装置７００がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

また、本実施の形態では図８及び図９において、メディア鍵で暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得したコンテンツ鍵でコンテンツを暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する１階層の構成であってもよい。また、記録装置内部で生成したコンテンツ鍵を用いてコンテンツを暗号化し、コンテンツ鍵をメディア鍵で暗号化し、暗号化コンテンツと暗号化コンテンツ鍵を記録媒体に記録する構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では鍵生成装置として図７に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではない。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、記録媒体への各データの記録は記録媒体製造機関に設置される装置で実行される形態であっても良い。一般的に書き換え型もしくは追記型の光ディスクでは、一般ユーザの保有する記録装置で記録可能な領域と、一般ユーザの保有する記録装置では記録不可能な再生専用領域を備えており、この再生専用領域にはディスク製造業者が出荷前にデータを記録する。この場合、ディスク製造業者による再生専用領域へのデータ記録は、スタンパと呼ばれる原盤にデータを記録し、このスタンパを用いたプレス工程で行われるのが一般的である。このようなディスク製造業者による再生

専用領域へのデータ記録工程において、暗号化メディア鍵データが記録媒体に記録される場合であっても本発明は適用可能である。

（実施の形態３）

本発明の実施の形態３は、実施の形態１と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。また、１枚の記録媒体に対して第１及び第２の２つのメディア鍵を用いて、第１カテゴリ及び第２カテゴリに属する再生装置において読み込まれる無効化データを記録媒体に記録することを特徴とする。

以下、本発明の実施の形態３について、図面を参照にしながら説明する。図１３は、コンテンツを暗号化して記録する記録装置１３００及び記録媒体１３２０を示しており、図１４は、記録媒体１３２０から暗号化コンテンツを読み出して復号する第１のカテゴリの再生装置１４００を示しており、図１５は、記録媒体１３２０から暗号化コンテンツを読み出して復号する第２のカテゴリの再生装置１５００を示している。また、図１６は記録媒体１３２０に記録される各種データの具体例を示している。

図１３の記録装置１３００が図１の記録装置１００と異なる点は、第１のカテゴリに対しては第１のメディア鍵を、第２のカテゴリに対しては第２のメディア鍵を、個別に設け、第１及び第２のメディア鍵をそれぞれ第１のメディア鍵暗号化部１３０５及び第２のメディア鍵暗号化部１３０６で暗号化し、コンテンツ鍵を第１及び第２のメディア鍵を用いてそれぞれ第１のコンテンツ鍵暗号化部１３０７及び第２のコンテンツ鍵暗号化部１３０８で暗号化し、記録媒体１３２０に記録するようにしたことである。その他の点は図１の記録装置１００と同じであるので、その説明は省略する。

記録媒体１３２０は、第１のメディア鍵暗号化部１３０５が生成した第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域１３２１と、第２のメディア鍵暗号化部１３０６が生成した第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域１３２２と、第１のコンテンツ鍵暗号化部１３０７が生成した第１の暗号化コンテンツ鍵を記録する第１の暗号化コンテンツ鍵記録領域１３２３と、第２のコンテンツ鍵暗号化部１３０８が生成した第２の暗号化コンテンツ鍵を記録する第２の暗号化コンテンツ鍵記録領域１３２４と、コンテンツ暗号化部１３０９が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域１３２５とを備える。

第１カテゴリの再生装置１４００及び第２のカテゴリの再生装置１５００は、それぞれ記録媒体１３２０から読み出した第１および第２の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する。その他の点については、実施の形態１における第１のカテゴリの再生装置２００及び第２のカテゴリの再生装置３００と同様であるので、その説明は省略する。

図１６は、ｍ台の第１のカテゴリの再生装置及びｎ台の第２のカテゴリの再生装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの再生装置２と第２のカテゴリの再生装置３が無効化されているとした場合の、記録媒体１３２０に記録される各種データの具体例を示している。図１６中で、第１のカテゴリの再生装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの再生装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＢｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）、Ｅｄ（Ｘ，Ｙ）及びＥｅ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長５６ｂｉｔのＤＥＳ暗号を使用した。

（第１の暗号化メディア鍵データ記録領域１３２１）

第１の暗号化メディア鍵データ記録領域１３２１には、第１のカテゴリの再生装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化された第１のメディア鍵（ＭＫ１）が記録されている。ここで、第１のカテゴリの再生装置２は無効化されており、ＤＫＡ２では第１のメディア鍵（ＭＫ１）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第１の暗号化メディア鍵データを生成する際に、第１のメディア鍵暗号化部１３０５において、第１のカテゴリのうち無効化すべき再生装置の情報として再生装置２が入力され、再生装置２では正しいメディア鍵が得られないように処理された結果である。第１の暗号化メディア鍵データをこのように生成することにより、再生装置２を除く第１のカテゴリの再生装置が正しい第１のメディア鍵（ＭＫ１）を復号することができ、再生装置２をシステムから排除することができる。

（第２の暗号化メディア鍵データ記録領域１３２２）

第２の暗号化メディア鍵データ記録領域１３２２には、第２のカテゴリの再生装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｎ）で暗号化された第２のメディア鍵（ＭＫ２）が記録されている。ここで、第２のカテゴリの再生装置３は無効化されており、ＤＫＢ３では第２のメディア鍵（ＭＫ２）とはまったく無関係のデータ「０」が暗号化されて記録されている。これは第２の暗号化メディア鍵データを生成する際に、第２のメディア鍵暗号化部１３０６において、第２のカテゴリのうち無効化すべき再生装置の情報として再生装置３が入力され、再生装置３では正しいメディア鍵が得られないように処理された結果である。第２の暗号化メディア鍵データをこのように生成することにより、再生装置３を除く第２のカテゴリの再生装置が正しい第２のメディア鍵（ＭＫ２）を復号することができ、再生装置３をシステムから排除することができる。

（第１の暗号化コンテンツ鍵記録領域１３２３）

第１の暗号化コンテンツ鍵記録領域１３２３には第１のメディア鍵（ＭＫ１）で暗号化されたコンテンツ鍵（ＣＫ）が記録されている。

（第２の暗号化コンテンツ鍵記録領域１３２４）

第２の暗号化コンテンツ鍵データ記録領域１３２４には第２のメディア鍵（ＭＫ２）で暗号化されたコンテンツ鍵（ＣＫ）が記録されている。

（暗号化コンテンツ記録領域１３２５）

暗号化コンテンツ記録領域１３２５には、コンテンツ鍵（ＣＫ）で暗号化されたコンテンツが記録されている。

以上のように構成された本発明の実施の形態１において、例えば第１のカテゴリの再生装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵及び第１の暗号化コンテンツ鍵を復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの再生装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの再生装置の無効化システムを更新することになる。以下、その具体例を説明する。

（システム更新の具体例１）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１３２０に記録する各種データの具体例１を図１７に示す。図１６との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析

行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図１７の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ１）を取得することはできず、コンテンツを再生することはできない。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。

（システム更新の具体例２）

第１のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１３２０に記録する各種データの具体例２を図１８に示す。図１６との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したこと、第１の暗号化メディア鍵データの暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したこと、第１の暗号化コンテンツ鍵の暗号化アルゴリズムをＥｃ（Ｘ，Ｙ）からＥｃ’（Ｘ，Ｙ）に変更したことである。ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっている。

一方、無効化されていない第１のカテゴリの各再生装置１４００には、新たなデバイス鍵を付与されデバイス鍵格納部１４０１に格納される。メディア鍵復号部１４０２には、以前から組み込まれている図１６の第１の暗号化メディア鍵を復号するための復号アルゴリズムＤａ（Ｘ，Ｙ）に加えて、図１８の第１の暗号化メディア鍵を復号するための復号アルゴリズムＤａ’（Ｘ，Ｙ）が組み込まれる。また、コンテンツ鍵復号部１４０３には、以前から組み込まれている図１６の第１の暗号化コンテ

ンツ鍵を復号するための復号アルゴリズムＤｃ（Ｘ，Ｙ）に加えて、図１８の第１の暗号化コンテンツ鍵を復号するための復号アルゴリズムＤｃ’（Ｘ，Ｙ）が組み込まれる。例えば、第１のカテゴリの再生装置ｍは、以前から保有していたデバイス鍵（ＤＫＡｍ）に加え、新たに付与されたデバイス鍵（ＤＫＡ’ｍ）を保有する。再生装置ｍは、図１６の記録媒体を再生する際には、デバイス鍵ＤＫＡｍと暗号化アルゴリズムＤａ（Ｘ，Ｙ）を用いて、第１の暗号化メディア鍵データを復号して第１のメディア鍵（ＭＫ１）を取得し、取得した第１のメディア鍵（ＭＫ１）と暗号化アルゴリズムＤｃ（Ｘ，Ｙ）を用いて第１の暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号する。一方、図１８の記録媒体を再生する際には、デバイス鍵ＤＫＡ’ｍと暗号アルゴリズムＤａ’（Ｘ，Ｙ）を用いて、第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ１）を取得し、取得したメディア鍵（ＭＫ１）と暗号化アルゴリズムＤｃ’（Ｘ，Ｙ）を用いて第１の暗号化コンテンツ鍵を復号してコンテンツ鍵（ＣＫ）を取得し、取得したコンテンツ鍵（ＣＫ）を用いて暗号化コンテンツを復号する。本実施の形態ではＥａ（Ｘ，Ｙ）、Ｄａ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）及びＤｃ（Ｘ，Ｙ）は鍵長５６ｂｉｔのＤＥＳ暗号を用いたのに対して、Ｅａ’（Ｘ，Ｙ）、Ｄａ’（Ｘ，Ｙ）、Ｅｃ’（Ｘ，Ｙ）及びＤｃ’（Ｘ，Ｙ）、では２キートリプルＤＥＳと呼ばれる鍵長１１２ｂｉｔの暗号を用いた。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図１８の記録媒体から読み出した第１の暗号化

メディア鍵データを復号してメディア鍵（ＭＫ１）を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）、第２の暗号化メディア鍵データの暗号化アルゴリズム、及び第２の暗号化コンテンツ鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する再生装置には何らの変更を加える必要がない。

以上のように構成された本発明の実施の形態３によれば、第１のカテゴリの再生装置１４００及び第２のカテゴリの再生装置１５００は、それぞれ異なるカテゴリの再生装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データ及び第１の暗号化コンテンツ鍵の生成に用いる暗号化アルゴリズムを、それぞれ第２の暗号化メディア鍵データ及び第２の暗号化コンテンツ鍵の生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの再生装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの再生装置に影響を与えることなく、無効化システムを変更することが可能になる。

また、本実施の形態では第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。す

なわち第１のカテゴリに属する再生装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第１のメディア鍵のみであり、第２のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。

なお、図１３では、第１のメディア鍵、第２のメディア鍵及びコンテンツ鍵が記録装置１３００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置１３００が第１のメディア鍵、第２のメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置１３００が第１のメディア鍵、第２のメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

また、図１３では、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を第１及び第２のメディア鍵で暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図１３に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではい。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部（図１３中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用す

る機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図１７のＥａ（ＤＫＡ’２，０）や図１８のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する再生装置の台数を増やすことが可能となる。

また、本実施の形態では、図１６に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

（実施の形態４）

本発明の実施の形態４は、実施の形態１と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。また、本実施の形態４に係る記録装置は、第１のコンテンツ鍵及び第２のコンテンツ鍵を用いてコンテンツを２回暗号化するものである。

以下、本発明の実施の形態４について、図面を参照にしながら説明する。図１９は、コンテンツを暗号化して記録する記録装置１９００及び記録媒体１９２０を示しており、図２０は、記録媒体１９２０から暗号化コンテンツを読み出して復号する第１の再生装置２０００を示しており、図２１は、記録媒体１９２０から暗号化コンテンツを読み出して復号する第２の再生装置２１００を示している。また、図２２は記録媒体１９２０に記録される各種データの具体例を示している。

図１９の記録装置１９００が図１の記録装置１００と異なる点は、コンテンツに対して第１のコンテンツ鍵を用いて第１のコンテンツ暗号化部１９０９で第１のコンテンツ暗号化を施し、その出力に対して第２のコンテンツ鍵を用いて第２のコンテンツ暗号化部１９１０で第２のコンテンツ暗号化を施し、メディア鍵を用いて第１及び第２のコンテンツ鍵

をそれぞれ第１のコンテンツ鍵暗号化部１９０７及び第２のコンテンツ鍵暗号化部１９０８で暗号化し、記録媒体１９２０に記録するようにしたことである。その他の点は図１の記録装置１００と同じであるので、その説明は省略する。

記録媒体１９２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域１９２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域１９２２と、第１のコンテンツ鍵暗号化部１９０７が生成した第１の暗号化コンテンツ鍵を記録する第１の暗号化コンテンツ鍵記録領域１９２３と、第２のコンテンツ鍵暗号化部１９０８が生成した第２の暗号化コンテンツ鍵を記録する第２の暗号化コンテンツ鍵記録領域１９２４と、第２のコンテンツ暗号化部１９１０が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域１９２５とを備える。

ＰＣ等の第１の再生装置２０００は、例えばドライブ装置である読み出し装置２０１０、及び、例えばアプリケーションでコンテンツの復号を実現する復号装置２０２０から構成される。そして、本実施の形態４においては、ドライブ装置等の読み出し装置２０１０においても暗号化コンテンツの復号化を行うことを特徴としている。

読み出し装置２０１０は、デバイス鍵を秘密に保有するデバイス鍵格納部２０１１と、デバイス鍵を用いて記録媒体１９２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得する第２のメディア鍵復号部２０１２と、取得したメディア鍵を用いて記録媒体から読み出した第２の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する第２のコンテンツ鍵復号部２０１３と、取得したコンテンツ鍵を用いて記録媒体１９２０から読み出した暗号化コンテンツに第２のコンテンツ復号処理を施す第２のコンテンツ復号部２０１４とを備え、第２の

コンテンツ復号部２０１４で暗号化コンテンツに第２の復号処理を施した結果の中間データを記録媒体１９２０から読み出した第１の暗号化メディア鍵データ及び第１の暗号化コンテンツ鍵とともに復号装置２０２０に供給する。本実施の形態において、読み出し装置２０１０は上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

復号装置２０２０は、デバイス鍵を秘密に保有するデバイス鍵格納部２０２１と、デバイス鍵を用いて読み出し装置２０１０から供給される第１の暗号化メディア鍵データを復号してメディア鍵を取得する第１のメディア鍵復号部２０２２と、取得したメディア鍵を用いて読み出し装置２０１０から供給される第１の暗号化コンテンツ鍵を復号して第１のコンテンツ鍵を取得する第１のコンテンツ鍵復号部２０２３と、取得した第１のコンテンツ鍵を用いて読み取り装置２０１０から供給される中間データに第１のコンテンツ復号処理を施してコンテンツを取得する第１のコンテンツ復号部２０２４とを備える。本実施の形態において、復号装置２０２０は上記した構成要素がソフトウェアで実装されており、第１のカテゴリに属するものとした。

第２の再生装置２１００は、第２のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部２１０１と、デバイス鍵を用いて記録媒体１９２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部２１０２と、取得したメディア鍵を用いて記録媒体から読み出した第２の暗号化コンテンツ鍵を復号して第２のコンテンツ鍵を取得する第２のコンテンツ鍵復号部２１０３と、取得した第２のコンテンツ鍵を用いて記録媒体１９２０から読み出した暗号化コンテンツに第２のコンテンツ復号処理を施す第２のコンテンツ復号部２１０４と、取得したメディア鍵を用いて記録媒体か

ら読み出した第１の暗号化コンテンツ鍵データを復号して第１のコンテンツ鍵を取得する第１のコンテンツ鍵復号部２１０５と、第２のコンテンツ復号部２１０４の出力に第１のコンテンツ鍵を用いて第１のコンテンツ復号処理を施してコンテンツを取得する第１のコンテンツ復号部２１０６とを備える。本実施の形態において、第２の再生装置２１００は、上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第１のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光ディスクドライブのようにハードウェアで実装される装置を第２のカテゴリに属する装置とした。

図２２は、ｍ台の第１のカテゴリの復号装置及びｎ台の第２のカテゴリの装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの復号装置２と第２のカテゴリの装置３が無効化されているとした場合の、記録媒体１９２０に記録される各種データの具体例を示している。図２２中で、第１のカテゴリの復号装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＡｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）、Ｅｄ（Ｘ，Ｙ）、Ｅｅ（Ｘ，Ｙ）及びＥｆ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

第１の暗号化メディア鍵データ記録領域１９２１及び第２の暗号化メディア鍵データ記録領域１９２２に記録されるデータは、それぞれ、前記した実施の形態１における第１の暗号化メディア鍵データ記録領域１

２１及び第２の暗号化メディア鍵データ記録領域１２２に記録されるデータと同じであるので、その説明は省略する。

（第１の暗号化コンテンツ鍵記録領域１９２３）

第１の暗号化コンテンツ鍵記録領域１９２３にはメディア鍵（ＭＫ）で暗号化された第１のコンテンツ鍵（ＣＫ１）が記録されている。

（第２の暗号化コンテンツ鍵記録領域１９２４）

第２の暗号化コンテンツ鍵記録領域１９２４にはメディア鍵（ＭＫ）で暗号化された第２のコンテンツ鍵（ＣＫ２）が記録されている。

（暗号化コンテンツ記録領域１９２５）

暗号化コンテンツ記録領域１９２５には、第１のコンテンツ鍵（ＣＫ１）及び第２のコンテンツ鍵（ＣＫ２）で暗号化されたコンテンツが記録されている。

以上のように構成された本発明の実施の形態４において、例えば第１のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

（システム更新の具体例１）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１９２０に記録する各種データの具体例１を図２３に示す。図２２との違いは、第１の暗号化メディア鍵の生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デ

バイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図２３の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。

（システム更新の具体例２）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体１９２０に記録する各種データの具体例２を図２４に示す。図２２との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例２と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図２４の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）及び第２の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。

以上のように構成された本発明の実施の形態４によれば、第１のカテゴリの装置（復号装置２０２０）及び第２のカテゴリの装置（読み出し装置２０１０及び第２の再生装置２１００）は、それぞれ異なるカテゴリの装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの復号装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。さらに、第１のカテゴリの復号装置２０２０には、第２の暗号化コンテンツ鍵を復号するためのアルゴリズムは実装されていないので、第１のカテゴリの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツの復号に必要な全ての情報を取得することはできず、より堅牢な著作権保護システムを構築できる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難な

ソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

なお、図１９で、メディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵が記録装置１９００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置１９００がメディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置１９００がメディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

また、図１９では、コンテンツを第１及び第２のコンテンツ鍵で暗号化し、第１及び第２のコンテンツ鍵をメディア鍵で暗号化する２階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図１９に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図１９中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第１の暗号化メディア

鍵データを生成する際に、図２３のＥａ（ＤＫＡ’２，０）や図２４のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

また、本実施の形態では、図２２に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

また、図２２では、コンテンツ全体を第１のコンテンツ鍵（ＣＫ１）で暗号化した後、さらに第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第１のコ

ンテンツ鍵（ＣＫ１）で暗号化し、他のブロックを第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしてもよい。

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

（実施の形態５）

本発明の実施の形態５は、実施の形態４のシステムにおいて、第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第１の暗号化コンテンツ鍵の階層を設けるようにしたものである。

そして、本実施の形態５においては、第１のメディア鍵及び第２のメディア鍵、第１のコンテンツ鍵及び第２のコンテンツ鍵を用いると共に、実施の形態４の再生装置２０００の構成に、新たに第２の再生装置を加えることを特徴としている。

以下、本発明の実施の形態５について、図面を参照しながら説明する。図２５は、コンテンツを暗号化して記録する記録装置２５００及び記録媒体２５２０を示しており、図２６は、記録媒体２５２０から暗号化コンテンツを読み出して復号する第１の再生装置２６００を示しており、図２７は、記録媒体２５２０から暗号化コンテンツを読み出して復号する第２の再生装置２７００を示している。また、図２８は記録媒体２５２０に記録される各種データの具体例を示している。

図２５の記録装置２５００が図１９の記録装置１９００と異なる点は、第１のカテゴリに対しては第１のメディア鍵を、第２のカテゴリに対しては第２のメディア鍵を、個別に設け、第１及び第２のメディア鍵をそれぞれ第１のメディア鍵暗号化部２５０５及び第２のメディア鍵暗号化部２５０６で暗号化し、第１のコンテンツ鍵を第１及び第２のメディア鍵を用いてそれぞれ第１コンテンツ鍵暗号化部（１）２５０７及び第１のコンテンツ鍵暗号化部（２）２５１１で暗号化し、記録媒体２５２０に記録するようにしたことである。その他の点については、前記した実施の形態４の記録装置１９００と同じであるので、その説明は省略する。

記録媒体２５２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域２５２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域２５２２と、第１のコンテンツ鍵暗号化部（１）２５０７が生成した第１の暗号化コンテンツ鍵（１）を記録する第１の暗号化コンテンツ鍵（１）記録領域２５２３と、第１のコンテンツ鍵暗号化部（２）２５１１が生成した第１の暗号化コンテンツ鍵（２）を記録する第１の暗号化コンテンツ鍵（２）記録領域２５２６と、第２の暗号化コンテンツ鍵を記録する第２の暗号化コンテンツ鍵記録領域２５２４と、暗号化コンテンツを記録する暗号化コンテンツ記録領域２５２５とを備える。

第１の再生装置２６００において復号装置２６２０は、読み出し装置２６１０が記録媒体２５２０から読み出した第１の暗号化コンテンツ鍵（１）を復号して第１のコンテンツ鍵を取得する。その他の点については、前記した実施の形態４における第１の再生装置２０００と同様であるので、その説明は省略する。

第２の再生装置２７００は、記録媒体２５２０から読み出した第１の暗号化コンテンツ鍵（２）を復号して第１のコンテンツ鍵を取得する。

その他の点については、前記した実施の形態４における第２の再生装置２１００と同様であるので、その説明は省略する。

図２８は、記録媒体２５２０に記録される各種データの具体例を示している。第１の暗号化メディア鍵データ記録領域２５２１には、第１のカテゴリの復号装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化された第１のメディア鍵（ＭＫ１）が記録されており、第２の暗号化メディア鍵データ記録領域２５２２には、第２のカテゴリの装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｍ）で暗号化された第２のメディア鍵（ＭＫ２）が記録されている。また、第１の暗号化コンテンツ鍵（１）記録領域２５２３には、第１のメディア鍵（ＭＫ１）で暗号化された第１のコンテンツ鍵（ＣＫ１）が記録されており、第１の暗号化コンテンツ鍵（２）記録領域２５２６には、第２のメディア鍵（ＭＫ２）で暗号化された第１のコンテンツ鍵（ＣＫ１）が記録されている。その他の点については、前記した図２２と同じであるので、説明を省略する。なお、図２８中の、Ｅｇ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味し、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

以上のように構成された本発明の実施の形態５において、例えば第１のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵を復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

（システム更新の具体例１）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体２５２０に記録する各種データの具体例

１を図２９に示す。図２８との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

（システム更新の具体例２）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体２５２０に記録する各種データの具体例２を図３０に示す。図２２との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したこと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したこと、及び第１の暗号化コンテンツ鍵（１）の暗号化アルゴリズムをＥｃ（Ｘ，Ｙ）からＥｃ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態３で述べたシステム更新の具体例２と同様であるので、詳細についての説明は省略する。

以上のように構成された本発明の実施の形態５によれば、前記した実施の形態４同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第１のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第１のメディア鍵のみであり、第２のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新

や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

なお、図２５で、第１のメディア鍵、第２のメディア鍵、第１のコンテンツ鍵、及び第２のコンテンツ鍵が記録装置２５００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置２５００がこれらの鍵を格納する格納部を有する構成であってもよい。また、記録装置２５００がこれらの鍵をその都度生成する生成部を有する構成であってもよい。

また、図２５では、コンテンツを第１及び第２のコンテンツ鍵で暗号化し、第１及び第２のコンテンツ鍵をメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図２５に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図２５中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図２９のＥａ（ＤＫＡ’２，０）や図３０のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されて

いる復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

また、本実施の形態では、図２８に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

また、図２８では、コンテンツ全体を第１のコンテンツ鍵（ＣＫ１）で暗号化した後、さらに第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第１のコンテンツ鍵（ＣＫ１）で暗号化し、他のブロックを第２のコンテンツ鍵（ＣＫ２）で暗号化するようにしてもよい。

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

（実施の形態６）

本発明の実施の形態６は、実施の形態１と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

以下、本発明の実施の形態６について、図面を参照にしながら説明する。図３１は、コンテンツを暗号化して記録する記録装置３１００及び記録媒体３１２０を示しており、図３２は、記録媒体３１２０から暗号化コンテンツを読み出して復号する第１の再生装置３２００を示しており、図３３は、記録媒体３１２０から暗号化コンテンツを読み出して復号する第２の再生装置３３００を示している。また、図３４は記録媒体３１２０に記録される各種データの具体例を示している。

図３１の記録装置３１００が図１の記録装置１００と異なる点は、コンテンツ鍵生成部３１０９で外部から入力される第１及び第２のシードを用いてコンテンツ鍵を生成し、メディア鍵を用いて第１及び第２のシードをそれぞれ第１のシード暗号化部３１０７及び第２のシード暗号化部３１０８で暗号化して、記録媒体３１２０に記録するようにしたことである。その他の点は図１の記録装置１００と同じであるので、その説明は省略する。

記録媒体３１２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域３１２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域３１２２と、第１のシード暗号化部３１０７が生成した第１の暗号化シードを記録する第１の暗号化シード記録領域３１２３と、第２のシード暗号化部３１０８が生成した第２の暗号化シードを記録する第２の暗号化シード記録領域３１２４と、暗号化コンテンツを記録する暗号化コンテンツ記録領域３１２５とを備える。

第１の再生装置３２００は、読み出し装置３２１０及び復号装置３２２０とから構成される。

読み出し装置３２１０は、デバイス鍵を秘密に保有するデバイス鍵格納部３２１１と、デバイス鍵を用いて記録媒体３１２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得する第２のメディア鍵復号部３２１２と、取得したメディア鍵を用いて記録媒体から読み出した第２の暗号化シードを復号して第２のシードを取得する第２のシード復号部３２１３と、取得した第２のシードを、記録媒体３２２０から読み出した第１の暗号化メディア鍵データ、第１の暗号化シード、及び暗号化コンテンツとともに復号装置３２２０に供給する。本実施の形態において、読み出し装置３２１０は上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

復号装置３２２０は、デバイス鍵を秘密に保有するデバイス鍵格納部３２２１と、デバイス鍵を用いて読み出し装置３２１０から供給される第１の暗号化メディア鍵データを復号してメディア鍵を取得する第１のメディア鍵復号部３２２２と、取得したメディア鍵を用いて読み出し装置３２１０から供給される第１の暗号化シードを復号して第１のシードを取得する第１のシード復号部３２２３と、取得した第１のシードと読

み出し装置３２１０から供給される第２のシードを用いてコンテンツ鍵を生成するコンテンツ鍵生成部３２２４と、生成したコンテンツ鍵を用いて読み取り装置３２１０から供給される暗号化コンテンツを復号するコンテンツ復号部３２２５とを備える。本実施の形態６において、復号装置３２２０は上記した構成要素がソフトウェアで実装されており、第１のカテゴリに属するものとした。尚、第１のシード及び第２のシードをそれぞれ６４ビットとし、それぞれの上位２８ビットを、コンテンツ鍵生成部３１０９及び３２２４においてビット連結して、５６ビットのコンテンツ鍵を得る等の方法が考えられる。

第２の再生装置３３００は、第２のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部３３０１と、デバイス鍵を用いて記録媒体３１２０から読み出した第２の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部３３０２と、取得したメディア鍵を用いて記録媒体から読み出した第１の暗号化シードを復号して第１のシードを取得する第１のシード復号部３３０３と、取得したメディア鍵を用いて記録媒体３１２０から読み出した第２の暗号化シードを復号して第２のシードを取得する第２のシード復号部３３０４と、取得した第１のシードと第２のシードからコンテンツ鍵を生成するコンテンツ鍵生成部３３０５と、生成したコンテンツ鍵を用いて記録媒体３１２０から読み出した暗号化コンテンツを復号するコンテンツ復号部３３０６とを備える。本実施の形態６において、第２の再生装置３３００は上記した構成要素がハードウェアで実装されており、第２のカテゴリに属するものとした。

本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第１のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光

ディスクドライブのようにハードウェアで実装される装置を第２のカテゴリに属する装置とした。

図３４は、ｍ台の第１のカテゴリの復号装置及びｎ台の第２のカテゴリの装置がそれぞれ固有のデバイス鍵を１個だけ保有しており、第１のカテゴリの復号装置２と第２のカテゴリの装置３が無効化されているとした場合の、記録媒体３１２０に記録される各種データの具体例を示している。図３４中で、第１のカテゴリの復号装置ｉ（ｉ＝１～ｍ）が保有するデバイス鍵をＤＫＡｉ、第２のカテゴリの装置ｊ（ｊ＝１～ｎ）が保有するデバイス鍵をＤＫＡｊとしている。また、Ｅａ（Ｘ，Ｙ）、Ｅｂ（Ｘ，Ｙ）、Ｅｃ（Ｘ，Ｙ）、Ｅｄ（Ｘ，Ｙ）、及びＥｅ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

第１の暗号化メディア鍵データ記録領域３１２１及び第２の暗号化メディア鍵データ記録領域３１２２に記録されるデータは、それぞれ、前記した実施の形態１における第１の暗号化メディア鍵データ記録領域１２１及び第２の暗号化メディア鍵データ記録領域１２２に記録されるデータと同じであるので、その説明は省略する。

（第１の暗号化シード記録領域３１２３）

第１の暗号化シード記録領域３１２３にはメディア鍵（ＭＫ）で暗号化された第１のシード（ＳＤ１）が記録されている。

（第２の暗号化シード記録領域３１２４）

第２の暗号化シード記録領域３１２４にはメディア鍵（ＭＫ）で暗号化された第２のシード（ＳＤ２）が記録されている。

（暗号化コンテンツ記録領域３１２５）

暗号化コンテンツ記録領域３１２５には、コンテンツ鍵（ＣＫ）で暗

号化されたコンテンツが記録されている。

以上のように構成された本発明の実施の形態において、例えば第１のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

（システム更新の具体例１）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３１２０に記録する各種データの具体例１を図３５に示す。図３４との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図３５の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）は変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。

（システム更新の具体例２）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３１２０に記録する各種データの具体例２を図３６に示す。図３４との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例２と同様であるので、詳細についての説明は省略する。

ここで、新たなデバイス鍵（ＤＫＡ’１～ＤＫＡ’ｍ）のうちの各デバイス鍵は、システム更新前のデバイス鍵（ＤＫＡ１～ＤＫＡｍ）のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がＤＫＡ２以外に存在したとしても、そのデバイス鍵を使って図３６の記録媒体から読み出した第１の暗号化メディア鍵データを復号してメディア鍵（ＭＫ）を取得することはできず、コンテンツを再生することはできない。

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

なお、上記したシステム更新に際して、第２の暗号化メディア鍵データの生成に用いるデバイス鍵（ＤＫＢ１～ＤＫＢｎ）及び第２の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第２のカテゴリに属する装置には何らの変更を加える必要がない。

以上のように構成された本発明の実施の形態５によれば、第１のカテゴリの装置（復号装置３２２０）及び第２のカテゴリの装置（読み出し装置３２１０及び第２の再生装置３３００）は、それぞれ異なるカテゴ

リの装置を無効化するための第１もしくは第２の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第１の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの復号装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵データの生成アルゴリズムを変更することで、第２のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。さらに、第１のカテゴリの復号装置３２２０には、第２の暗号化シードを復号するためのアルゴリズムは実装されていないので、第１のカテゴリの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツ毎に異なる第２の暗号化シードを復号することはできず、第１のカテゴリに対する不正行為がシステム全体に影響することを防ぐことができ、より堅牢な著作権保護システムを構築できる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

なお、図３１で、メディア鍵、第１のシード、及び第２のシードが記録装置３１００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置３１００がメディア鍵、第１のシード、及び第２のシードを格納する格納部を有する構成であってもよい。また、記録装置３１００がメディア鍵、第１のシード、及び

第２のシードをその都度生成する生成部を有する構成であってもよい。

また、図３１では、第１のシード及び第２のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第１及び第２のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図３１に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部（図３１中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図３５のＥａ（ＤＫＡ’２，０）や図３６のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いるこ

とができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

また、本実施の形態では、図３４に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

（実施の形態７）

本発明の実施の形態７は、実施の形態６のシステムにおいて、第１のカテゴリと第２のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第１の暗号化シードの階層を設けるようにしたものである。

以下、本発明の実施の形態７について、図面を参照にしながら説明する。図３７は、コンテンツを暗号化して記録する記録装置３７００及び記録媒体３７２０を示しており、図３８は、記録媒体３７２０から暗号化コンテンツを読み出して復号する第１の再生装置３８００を示しており、図３９は、記録媒体３７２０から暗号化コンテンツを読み出して復号する第２の再生装置３９００を示している。また、図４０は記録媒体３７２０に記録される各種データの具体例を示している。

図３７の記録装置３７００が図３１の記録装置３１００と異なる点は、第１のカテゴリに対しては第１のメディア鍵を、第２のカテゴリに対しては第２のメディア鍵を、個別に設け、第１及び第２のメディア鍵をそれぞれ第１のメディア鍵暗号化部３７０５及び第２のメディア鍵暗号化部３７０６で暗号化し、第１のシードを第１及び第２のメディア鍵を用いてそれぞれ第１シード暗号化部（１）３７０７及び第１のシード暗号化部（２）３７１１で暗号化し、記録媒体３７２０に記録するようにしたことである。その他の点については、前記した実施の形態６の記録装置３１００と同じであるので、その説明は省略する。

記録媒体３７２０は、第１の暗号化メディア鍵データを記録する第１の暗号化メディア鍵データ記録領域３７２１と、第２の暗号化メディア鍵データを記録する第２の暗号化メディア鍵データ記録領域３７２２と、第１のシード暗号化部(１)３７０７が生成した第１の暗号化シード(１)を記録する第１の暗号化シード（１）記録領域３７２３と、第１のシード暗号化部（２）３７１１が生成した第１の暗号化シード（２）を記録する第１の暗号化シード（２）記録領域３７２６と、第２の暗号化シードを記録する第２の暗号化シードデータ記録領域３７２４と、暗号化コンテンツを記録する暗号化コンテンツ記録領域３７２５とを備える。尚、第２の暗号化シードデータは、第１の再生装置３８００の読み出し装置

３８１０及び第２の再生装置３９００において第２メディア鍵を用いて復号される。

第１の再生装置３８００において復号装置３８２０は、読み出し装置３８１０が記録媒体３７２０から読み出した第１の暗号化シード（１）を復号して第１のシードを取得する。その他の点については、前記した実施の形態６における第１の再生装置３２００と同様であるので、その説明は省略する。

第２の再生装置３９００は、記録媒体３７２０から読み出した第１の暗号化シード（２）を復号して第１のシードを取得する。その他の点については、前記した実施の形態６における第２の再生装置３３００と同様であるので、その説明は省略する。

図４０は、記録媒体３７２０に記録される各種データの具体例を示している。第１の暗号化メディア鍵データ記録領域３７２１には、第１のカテゴリの復号装置が保有するデバイス鍵（ＤＫＡ１～ＤＫＡｍ）で暗号化された第１のメディア鍵（ＭＫ１）が記録されており、第２の暗号化メディア鍵データ記録領域３７２２には、第２のカテゴリの装置が保有するデバイス鍵（ＤＫＢ１～ＤＫＢｍ）で暗号化された第２のメディア鍵（ＭＫ２）が記録されている。また、第１の暗号化シードデータ（１）記録領域３７２３には、第１のメディア鍵（ＭＫ１）で暗号化された第１のシード（ＳＤ１）が記録されており、第１の暗号化シードデータ（２）記録領域３７２６には、第２のメディア鍵（ＭＫ２）で暗号化された第１のシード（ＳＤ１）が記録されている。その他の点については、前記した図３４と同じであるので、説明を省略する。なお、図４０中の、Ｅｆ（Ｘ，Ｙ）はデータＹを鍵データＸを用いて暗号化する関数を意味し、本実施の形態では鍵長５６ビットのＤＥＳ暗号を使用した。

以上のように構成された本発明の実施の形態７において、例えば第１

のカテゴリの復号装置に付与したデバイス鍵の多数や、第１の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第１のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第１のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

（システム更新の具体例１）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３７２０に記録する各種データの具体例１を図４１に示す。図４０との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したことである。これは、前記した実施の形態１で述べたシステム更新の具体例１と同様であるので、詳細についての説明は省略する。

（システム更新の具体例２）

第１のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体３７２０に記録する各種データの具体例２を図４２に示す。図４０との違いは、第１の暗号化メディア鍵データの生成に用いるデバイス鍵をＤＫＡ１～ＤＫＡｍからＤＫＡ’１～ＤＫＡ’ｍに変更したこと、暗号化アルゴリズムをＥａ（Ｘ，Ｙ）からＥａ’（Ｘ，Ｙ）に変更したこと、及び第１の暗号化シード（１）の暗号化アルゴリズムをＥｃ（Ｘ，Ｙ）からＥｃ’（Ｘ，Ｙ）に変更したことである。これは、前記した実施の形態３で述べたシステム更新の具体例２と同様であるので、詳細についての説明は省略する。

以上のように構成された本発明の実施の形態７によれば、前記した実施の形態６同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第１のカテゴリと第２のカテゴリに対して個別にメデ

ィア鍵を設け、それぞれを用いた暗号化シードの階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第１のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第１のメディア鍵のみであり、第２のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第１のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第２のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

なお、図３７で、第１のメディア鍵、第２のメディア鍵、第１のシード、及び第２のシードが記録装置３７００の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置３７００がこれらを格納する格納部を有する構成であってもよい。また、記録装置３７００がこれらをその都度生成する生成部を有する構成であってもよい。

また、図３７では、第１のシード及び第２のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第１及び第２のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

また、本実施の形態では記録装置として図３７に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリの

デバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部（図３７中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

また、本実施の形態ではシステム更新において第１の暗号化メディア鍵データを生成する際に、図４１のＥａ（ＤＫＡ’２，０）や図４２のＥａ’（ＤＫＡ’２，０）のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第１の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第１のカテゴリに属する復号装置の台数を増やすことが可能となる。

また、本実施の形態では、図４０に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献１として開示されている木構造を利用した無効化方法を用いても良い。

また、本実施の形態では、暗号アルゴリズムとして鍵長５６ｂｉｔのＤＥＳ、あるいはシステム更新後の暗号アルゴリズムとして鍵長１１２

ｂｉｔの２キートリプルＤＥＳを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長１２８ｂｉｔのＡＥＳ等を用いても良い。

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態２のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

本発明によれば、第１のカテゴリの装置及び第２のカテゴリの装置は、それぞれ異なるカテゴリの装置を無効化するための第１もしくは第２の暗号化メディア鍵を読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。

また、第１の暗号化メディア鍵の生成に用いる暗号化アルゴリズムを第２の暗号化メディア鍵の生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第１のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第１のカテゴリの再生装置に付与するデバイス鍵の鍵長や第１の暗号化メディア鍵の生成アルゴリズムを変更することで、第２のカテゴリの再生装置に影響を与えることなく、無効化システムを更新することができる。

産業上の利用の可能性

本発明にかかる著作権保護システムは、装置内に設けるメモリのサイズを小さくでき、かつ、あるカテゴリの装置が不正に解析されてアルゴ

リズムや多数の鍵が暴露された場合にも、そのカテゴリの装置用の暗号化・復号のアルゴリズムや鍵長を変更することで、他のカテゴリの装置に何らの変更を加えることなく、システム全体の無効化機能を維持できるという効果があり、著作物をデジタル化したコンテンツを光ディスク等の大容量記録媒体に記録もしくは再生するシステムにおいて、復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される記録装置もしくは再生装置と、堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される記録装置もしくは再生装置とが存在するような場合に有用である。

請　求　の　範　囲

1．コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、

前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、

前記記録装置は、メディア鍵と前記Ｎ個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、

前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する

ことを特徴とする著作権保護システム。

2．前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、

前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得

し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項１記載の著作権保護システム。

３．前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化し、

前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項２記載の著作権保護システム。

４．前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、

前記各カテゴリの再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する

ことを特徴とする請求項２記載の著作権保護システム。

５．前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵を生成し、少なくとも前記Ｎ個の暗号化メディア鍵データと前記Ｎ

個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録し、

前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する

ことを特徴とする請求項１記載の著作権保護システム。

６．前記再生装置は、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第２のカテゴリに属する第２再生装置、及び、前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第２のカテゴリの読み出し装置と前記第２のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第１のカテゴリの復号装置とを備える第１再生装置から構成され、

前記記録装置は、メディア鍵と前記第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、少なくとも前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、

前記第２再生装置は、前記記録媒体から前記第２の無効化データ及び

前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号し、

前記第１再生装置において、前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記第１の無効化データを前記第１カテゴリの復号装置に供給し、前記第１のカテゴリの復号装置は、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施し前記コンテンツを取得する

ことを特徴とする請求項１記載の著作権保護システム。

７．コンテンツを暗号化して記録する記録装置であって、

前記記録装置は、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する

ことを特徴とする記録装置。

８．前記Ｎ個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データである

ことを特徴とする請求項７記載の記録装置。

９．前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化する

ことを特徴とする請求項８記載の記録装置。

１０．前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録する

ことを特徴とする請求項８記載の記録装置。

１１．前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化してＮ個の暗号化コンテンツ鍵データを生成し、少なくとも前記Ｎ個の暗号化メディア鍵データと前記Ｎ個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録する

ことを特徴とする請求項７記載の記録装置。

１２．前記記録装置は、メディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データを生成し、前記メディア鍵と前記第２のカテゴリの装置が保有するデバイス鍵データとから前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データを生成し、前記メディア鍵に基づいて

前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、少なくとも前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録する

ことを特徴とする請求項７記載の記録装置。

１３．暗号化コンテンツが記録される記録媒体であって、

前記記録媒体には、少なくとも、メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツが記録される

ことを特徴とする記録媒体。

１４．前記Ｎ個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データである

ことを特徴とする請求項１３記載の記録媒体。

１５．前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものである

ことを特徴とする請求項１４記載の記録媒体。

１６．前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録される

ことを特徴とする請求項１４記載の記録媒体。

１７．前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化して生成されたＮ個の暗号化コンテンツ鍵が記録される

ことを特徴とする請求項１３記載の記録媒体。

１８．前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとが記録される

ことを特徴とする請求項１３記載の記録媒体。

１９．記録媒体に記録された暗号化コンテンツを再生する再生装置であって、

前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されて

おり、

前記記録媒体には、少なくともメディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、

前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する

ことを特徴とする再生装置。

２０．前記Ｎ個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、

前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項１９記載の再生装置。

２１．前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであり、

前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項２０記載の再生装置。

２２．前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、

前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する

ことを特徴とする請求項２０記載の再生装置。

２３．前記Ｎ個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記コンテンツ鍵を前記Ｎ個のメディア鍵で暗号化して生成されたＮ個の暗号化コンテンツ鍵が記録されており、

前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号する

ことを特徴とする請求項１９記載の再生装置。

２４．前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記再生装置は、前記第２のカテゴリに属し、前記記録媒体から前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツを復号する

ことを特徴とする請求項１９記載の再生装置。

２５．記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、

前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記読み出し装置は、前記第２のカテゴリに属し、前記記録媒体から

前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第１の無効化データを出力する

ことを特徴とする読み出し装置。

２６．記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、

前記記録媒体には、少なくともメディア鍵と第１のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第１のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第１の無効化データと、前記メディア鍵と第２のカテゴリの装置が保有するデバイス鍵データとから生成された前記第２のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第２の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記第２のカテゴリの読み出し装置は、前記記録媒体から前記第１の無効化データ、前記第２の無効化データ及び前記暗号化コンテンツを読み出し、前記第２の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第１の無効化データを出力し、

前記復号装置は、前記第１のカテゴリに属し、前記第２のカテゴリの読み出し装置から供給される前記中間データに前記第１の無効化データに基づいて復号処理を施して前記コンテンツを取得する

ことを特徴とする復号装置。

２７．記録媒体に記録された暗号化コンテンツを再生する再生装置であって、請求項２５記載の読み取り装置と請求項２６記載の復号装置とから構成される

ことを特徴とする再生装置。

２８．コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツが記録された記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、

前記記録装置及び前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、

前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録し、

前記記録装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、

前記再生装置は、前記記録媒体から前記Ｎ個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する

ことを特徴とする著作権保護システム。

２９．メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記Ｎ個の各カテゴリに対してそれぞれ生成し、生成した前記Ｎ個の無効化データを前記記録媒体に記録する

ことを特徴とする鍵生成装置。

３０．コンテンツを暗号化して記録する記録装置であって、

メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録媒体から、前記Ｎ個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、

読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、

生成した前記暗号化コンテンツを前記記録媒体に記録する

ことを特徴とする記録装置。

３１．コンテンツを暗号化して記録する記録装置に用いる記録方法であって、

メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効

化データを前記Ｎ個の各カテゴリに対してそれぞれ生成する生成ステップと、

前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成する暗号化コンテンツ生成ステップと、

少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する記録ステップとを含む

ことを特徴とする記録方法。

３２．記録媒体に記録された暗号化コンテンツを再生する再生装置に用いる再生方法であって、

前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、

前記記録媒体には、少なくともメディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、

前記再生方法は、

前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み出しステップと、

前記読み出しステップにおいて読み出した前記無効化データに基づいて前記暗号化コンテンツを復号する復号ステップとを含む

ことを特徴とする再生方法。

３３．コンテンツを暗号化して記録する記録装置に用いるプログラム

であって、

メディア鍵とＮ個（Ｎは２以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記Ｎ個の各カテゴリに対してそれぞれ生成する生成ステップと、

前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成する暗号化コンテンツ生成ステップと、

少なくとも前記Ｎ個の無効化データと前記暗号化コンテンツを前記記録媒体に記録する記録ステップとを含む

ことを特徴とするプログラム。

３４．記録媒体に記録された暗号化コンテンツを再生する再生装置に用いるプログラムであって、

前記再生装置はＮ個（Ｎは２以上の自然数）のカテゴリに分類されており、

前記記録媒体には、少なくともメディア鍵と前記Ｎ個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、

前記プログラムは、

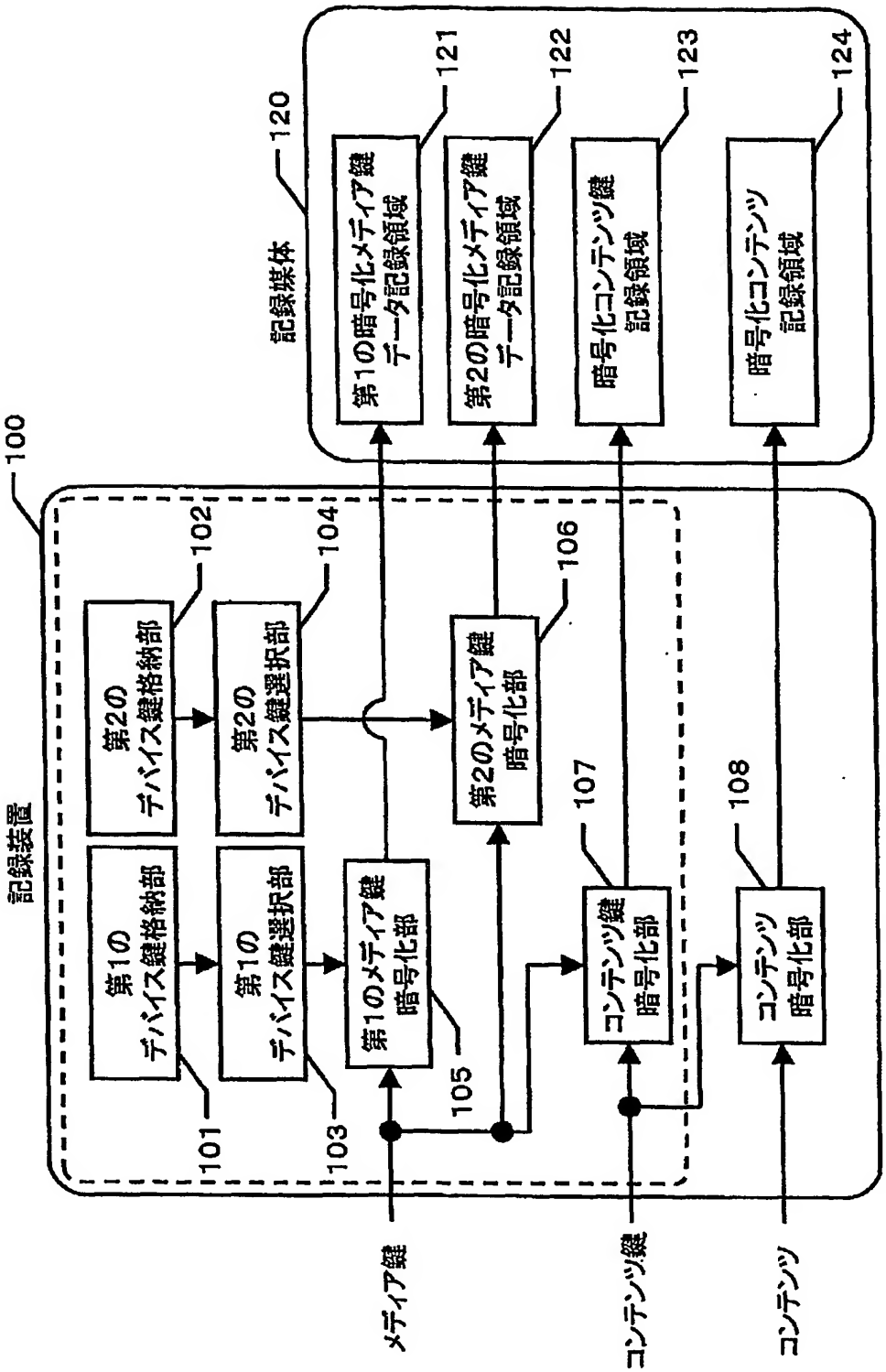
前記記録媒体から前記Ｎ個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出す読み出しステップと、

前記読み出しステップにおいて読み出した前記無効化データに基づい

て前記暗号化コンテンツを復号する復号ステップとを含む

ことを特徴とするプログラム。

図1



差替え用紙(規則26)

図2

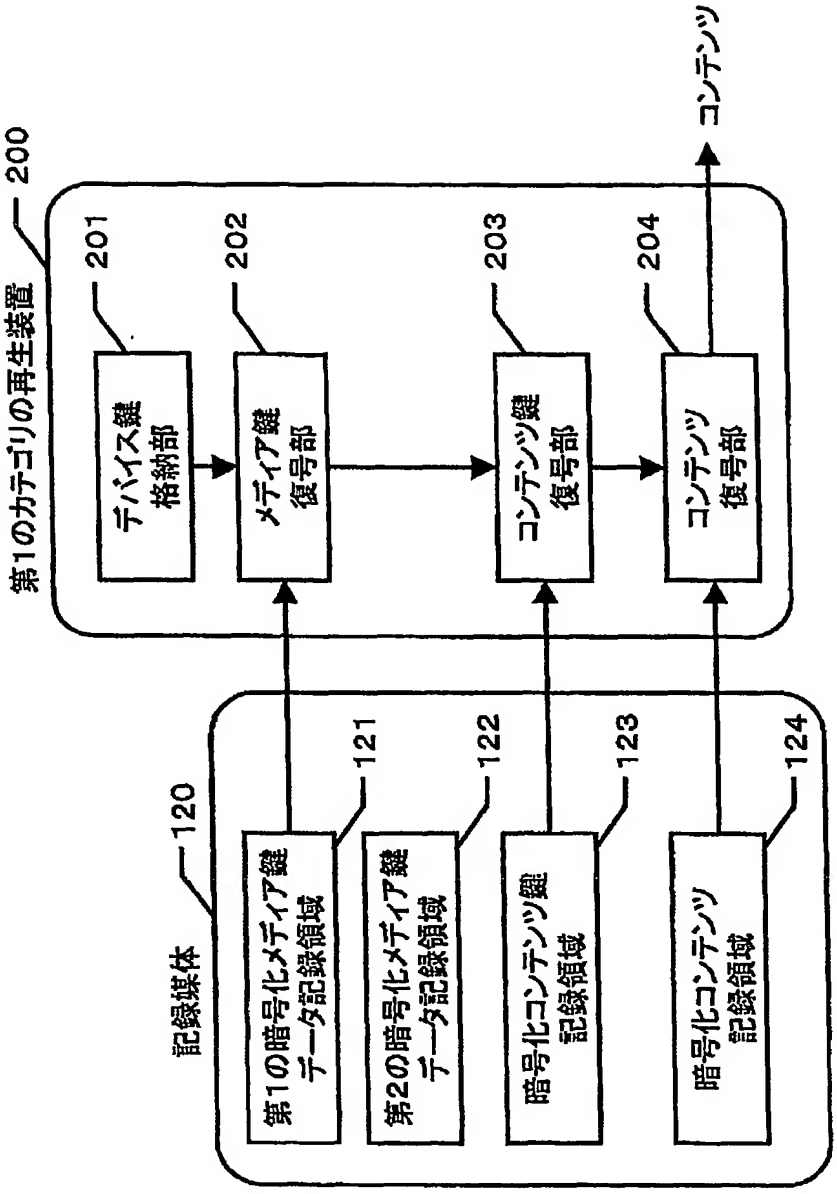

コンテンツ
200
第1のカテゴリの再生装置
201
デバイス鍵
格納部
202
メディア鍵
復号部
203
コンテンツ鍵
復号部
204
コンテンツ
復号部
120
記録媒体
121
第1の暗号化メディア鍵
データ記録領域
122
第2の暗号化メディア鍵
データ記録領域
123
暗号化コンテンツ鍵
記録領域
124
暗号化コンテンツ
記録領域

図3

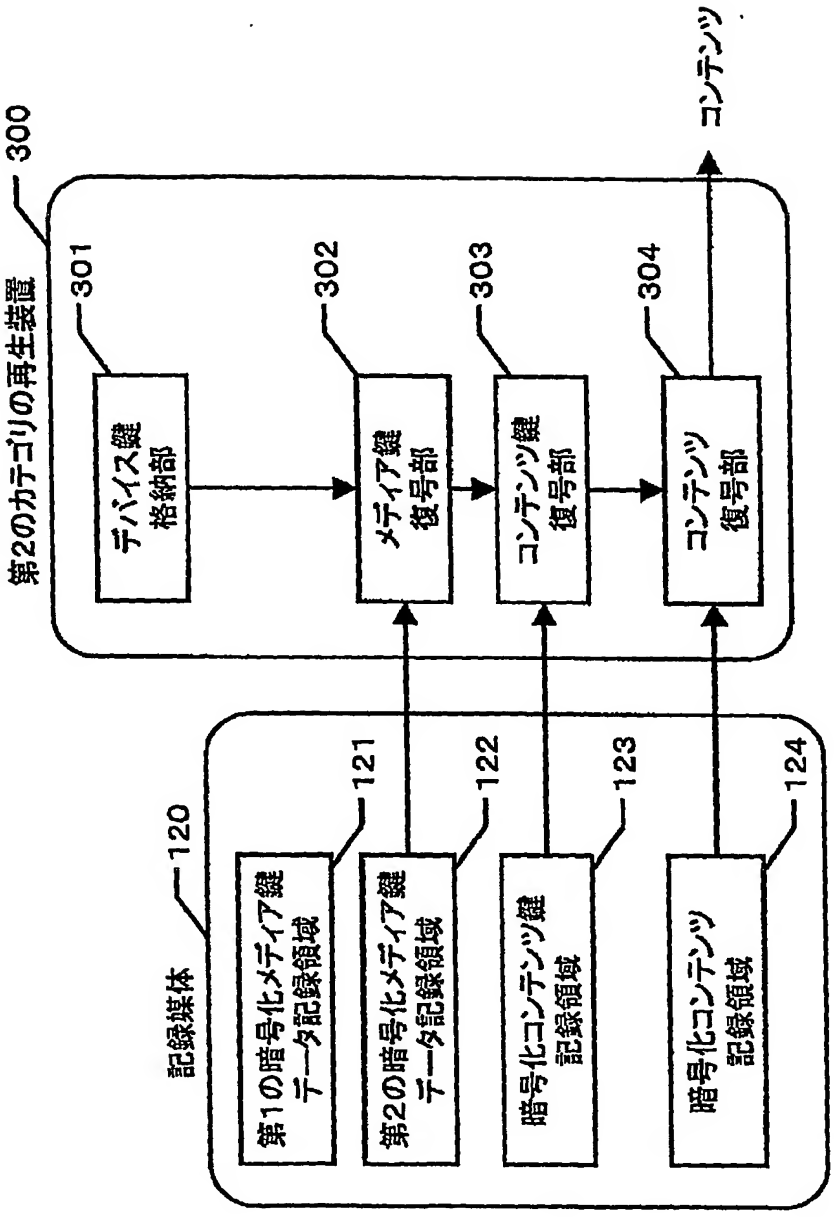

コンテンツ
300
第2のカテゴリの再生装置
301
デバイス鍵
格納部
302
メディア鍵
復号部
303
コンテンツ鍵
復号部
304
コンテンツ
復号部
記録媒体
120
121
第1の暗号化メディア鍵
データ記録領域
122
第2の暗号化メディア鍵
データ記録領域
123
暗号化コンテンツ鍵
記録領域
124
暗号化コンテンツ
記録領域

図4

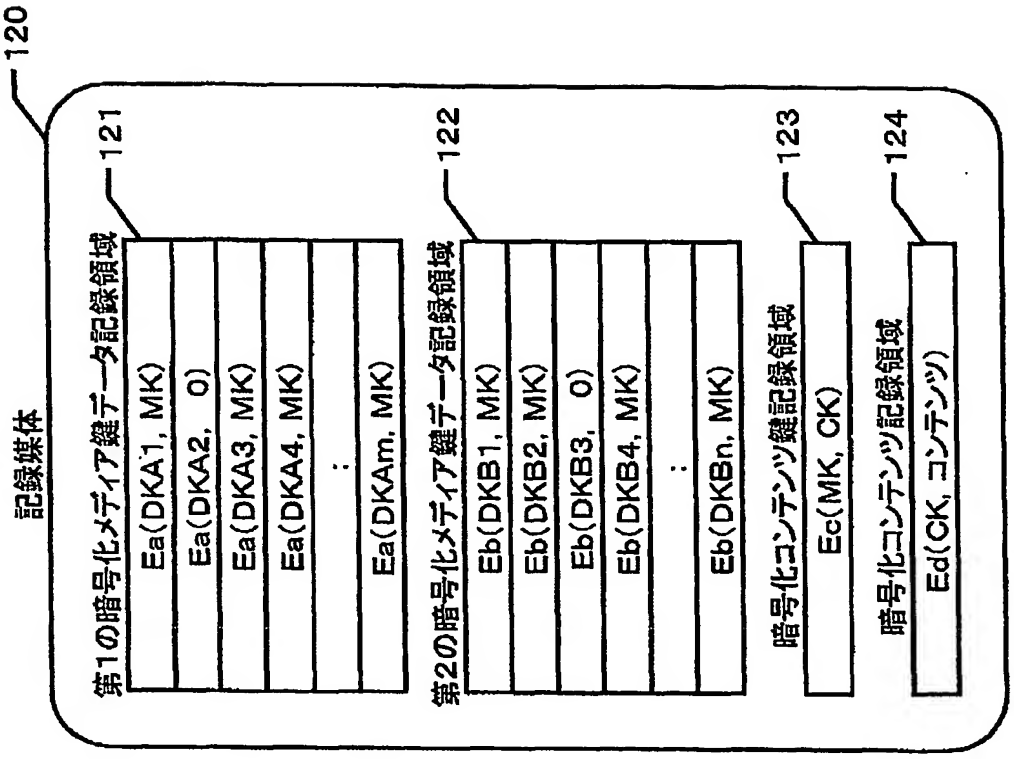

120
記録媒体
第1の暗号化メディア鍵データ記録領域
121
Ea(DKA1, MK)
Ea(DKA2, 0)
Ea(DKA3, MK)
Ea(DKA4, MK)
Ea(DKAm, MK)
第2の暗号化メディア鍵データ記録領域
122
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
暗号化コンテンツ鍵記録領域
123
Ec(MK, CK)
暗号化コンテンツ記録領域
124
Ed(CK, コンテンツ)

図5

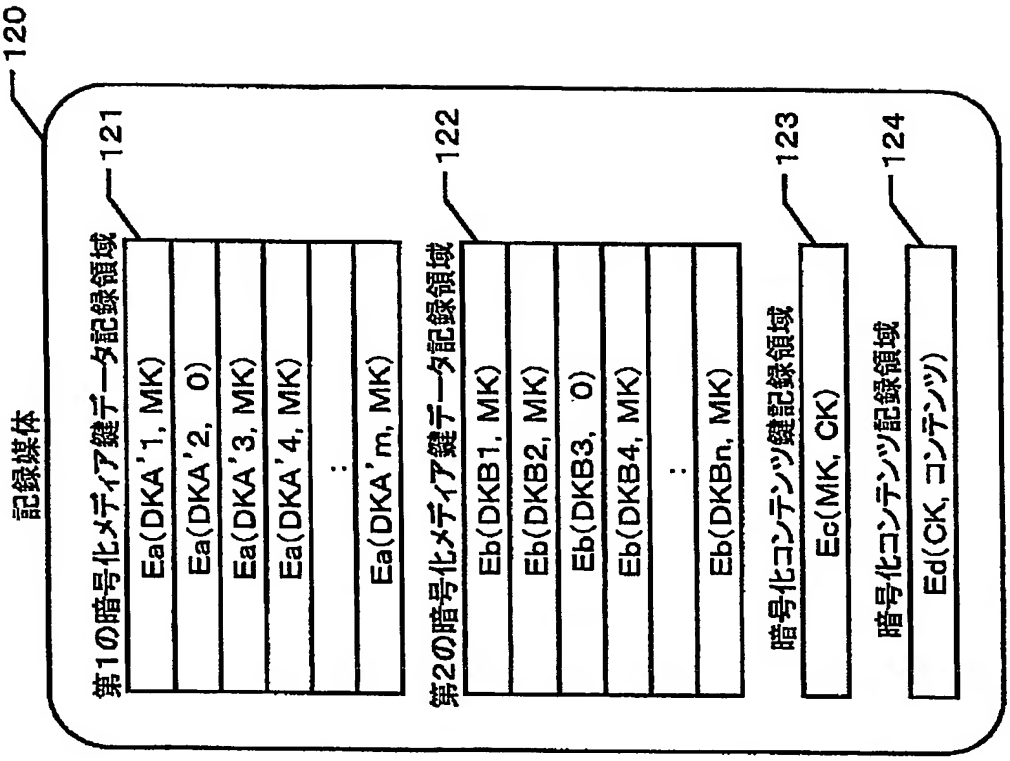

120
記録媒体
121
第1の暗号化メディア鍵データ記録領域
Ea(DKA'1, MK)
Ea(DKA'2, 0)
Ea(DKA'3, MK)
Ea(DKA'4, MK)
:
Ea(DKA'm, MK)
122
第2の暗号化メディア鍵データ記録領域
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
:
Eb(DKBn, MK)
123
暗号化コンテンツ鍵記録領域
Ec(MK, CK)
124
暗号化コンテンツ記録領域
Ed(CK, コンテンツ)

図6

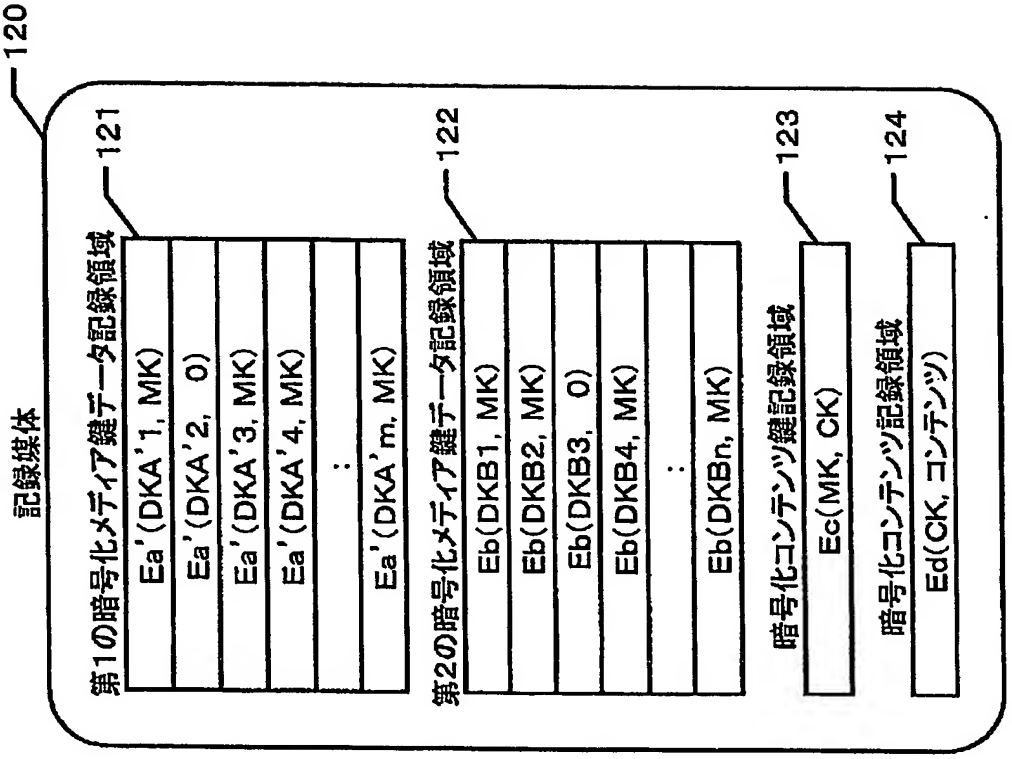
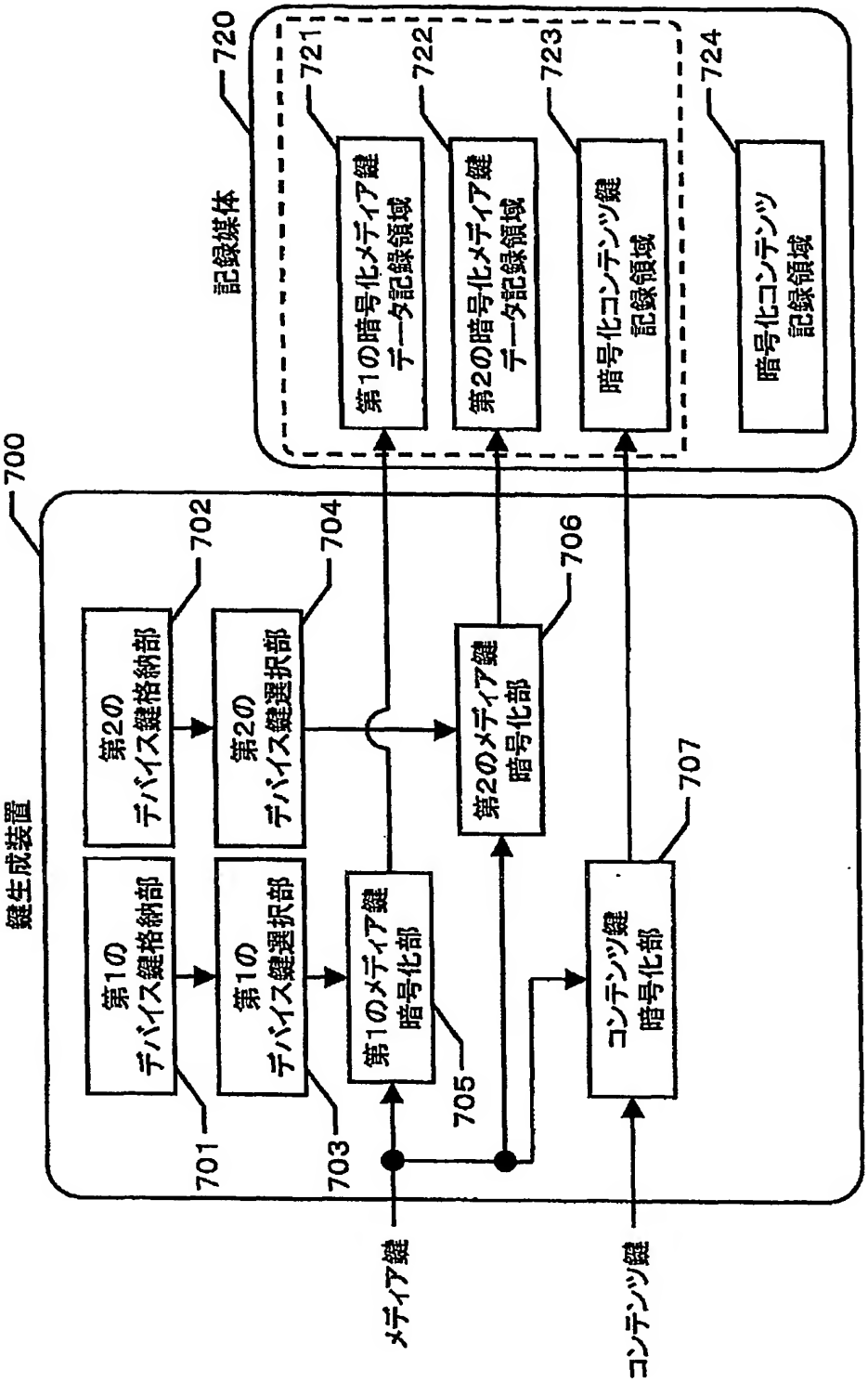

120
記録媒体
第1の暗号化メディア鍵データ記録領域
121
Ea'(DKA'1, MK)
Ea'(DKA'2, 0)
Ea'(DKA'3, MK)
Ea'(DKA'4, MK)
Ea'(DKA'm, MK)
第2の暗号化メディア鍵データ記録領域
122
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
暗号化コンテンツ鍵記録領域
123
Ec(MK, CK)
暗号化コンテンツ記録領域
124
Ed(CK, コンテンツ)

図7



差替え用紙(規則26)

図8

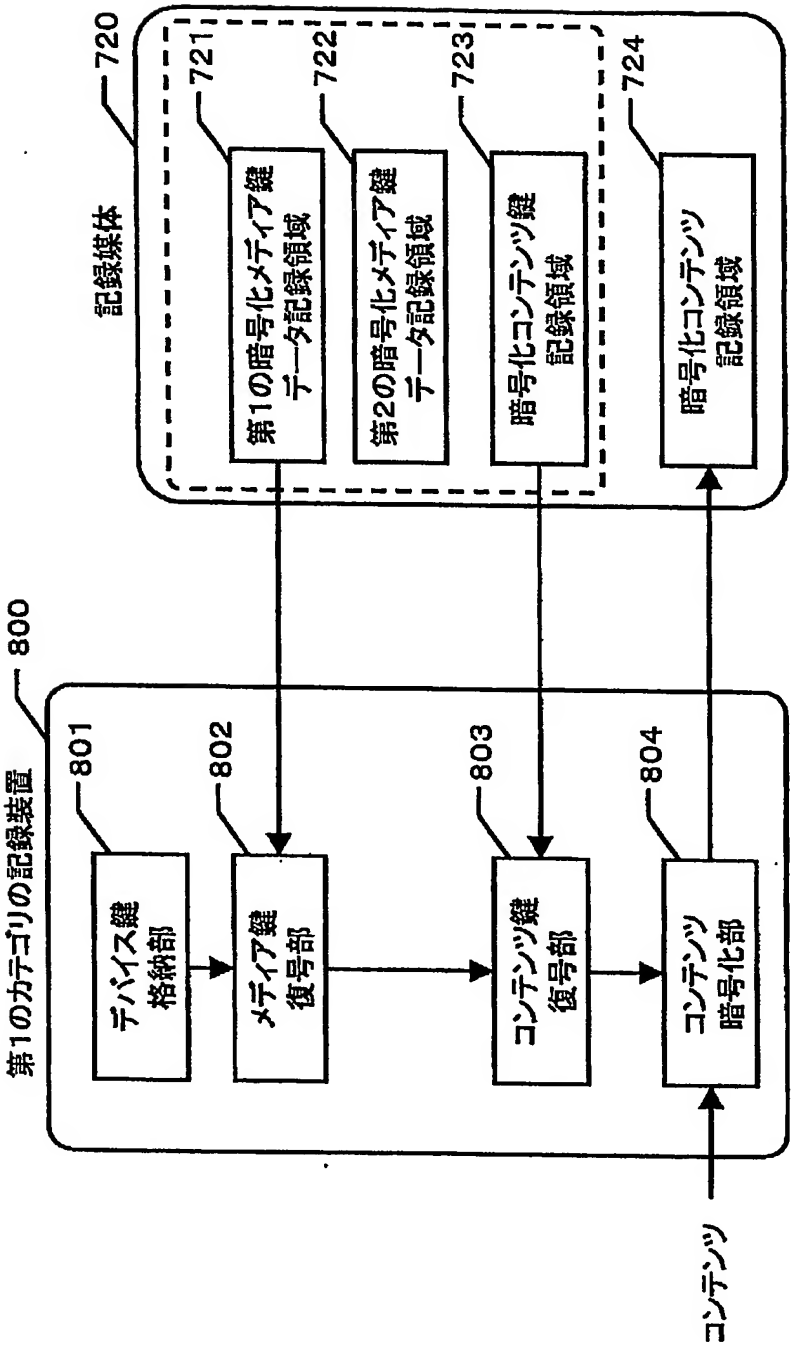

記録媒体
720
721
第1の暗号化メディア鍵
データ記録領域
722
第2の暗号化メディア鍵
データ記録領域
723
暗号化コンテンツ鍵
記録領域
724
暗号化コンテンツ
記録領域
第1のカテゴリの記録装置
800
801
デバイス鍵
格納部
802
メディア鍵
復号部
803
コンテンツ鍵
復号部
804
コンテンツ
暗号化部
コンテンツ

図9

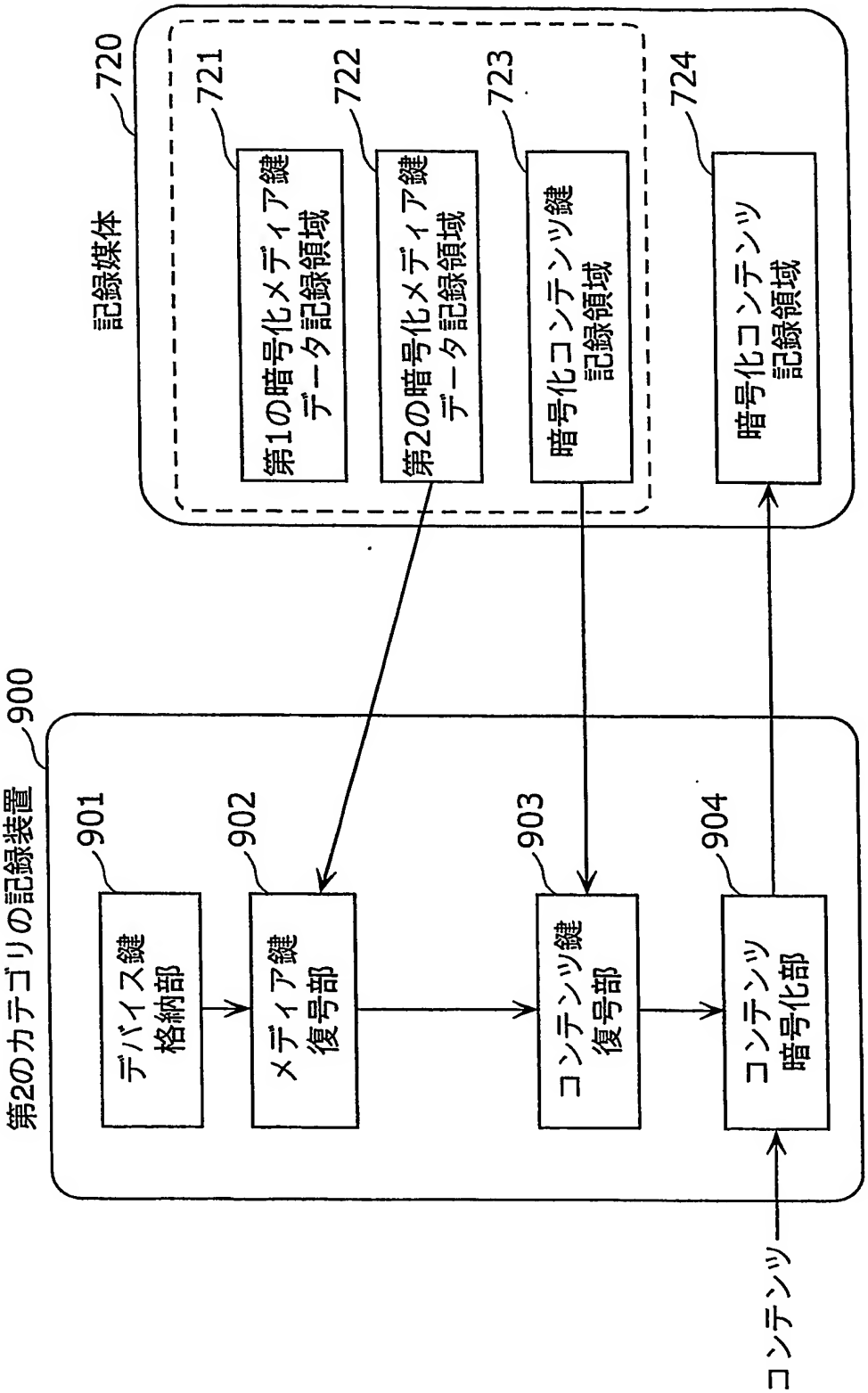

記録媒体
720
721
第1の暗号化メディア鍵データ記録領域
722
第2の暗号化メディア鍵データ記録領域
723
暗号化コンテンツ鍵記録領域
724
暗号化コンテンツ記録領域
第2のカテゴリの記録装置
900
901
デバイス鍵格納部
902
メディア鍵復号部
903
コンテンツ鍵復号部
904
コンテンツ暗号化部
コンテンツ

図10

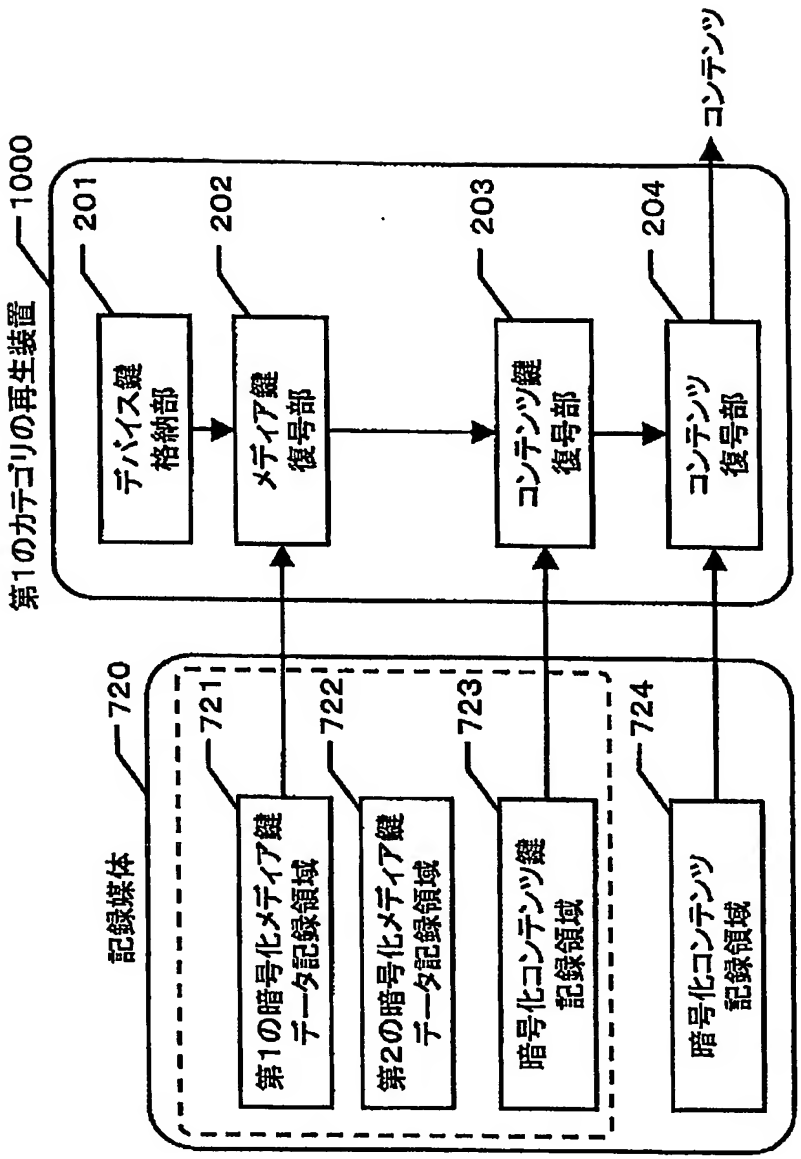

コンテンツ
第1のカテゴリの再生装置
1000
201
202
203
204
デバイス鍵
格納部
メディア鍵
復号部
コンテンツ鍵
復号部
コンテンツ
復号部
記録媒体
720
721
722
723
724
第1の暗号化メディア鍵
データ記録領域
第2の暗号化メディア鍵
データ記録領域
暗号化コンテンツ鍵
記録領域
暗号化コンテンツ
記録領域

図11

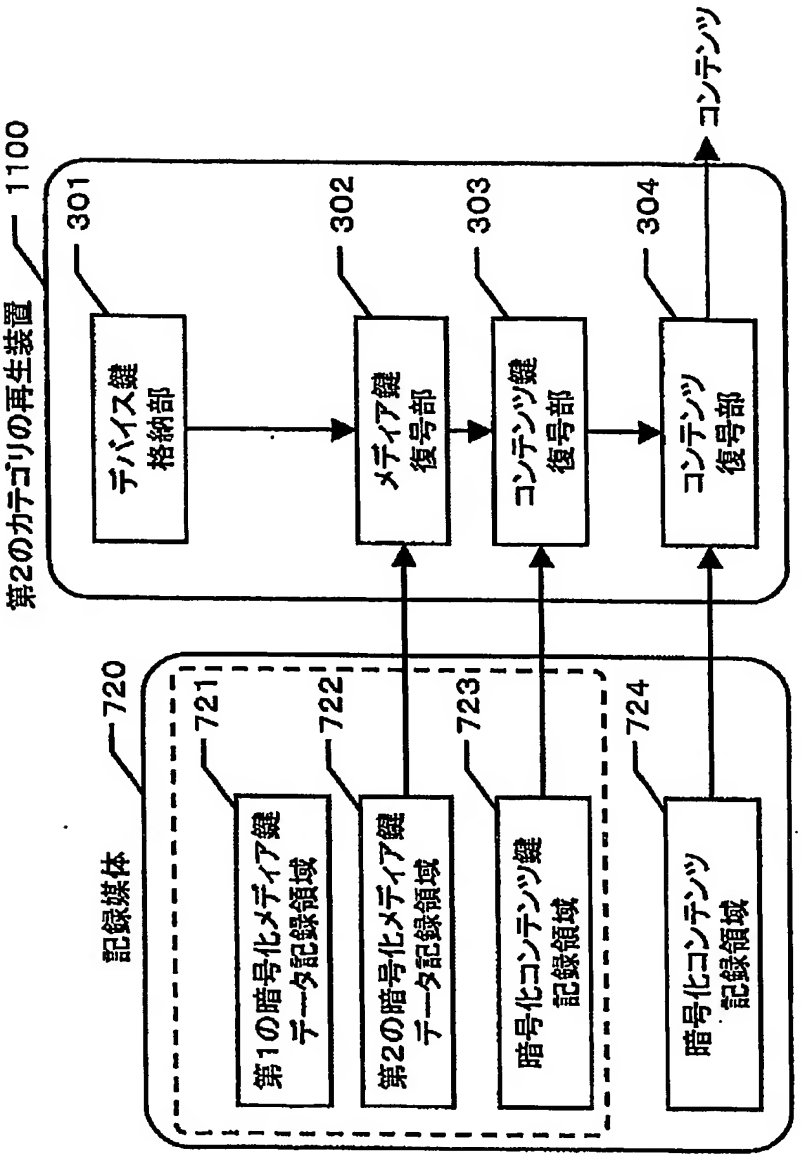

コンテンツ
第2のカテゴリの再生装置
1100
301
デバイス鍵
格納部
302
メディア鍵
復号部
303
コンテンツ鍵
復号部
304
コンテンツ
復号部
記録媒体
720
721
第1の暗号化メディア鍵
データ記録領域
722
第2の暗号化メディア鍵
データ記録領域
723
暗号化コンテンツ鍵
記録領域
724
暗号化コンテンツ
記録領域

図12

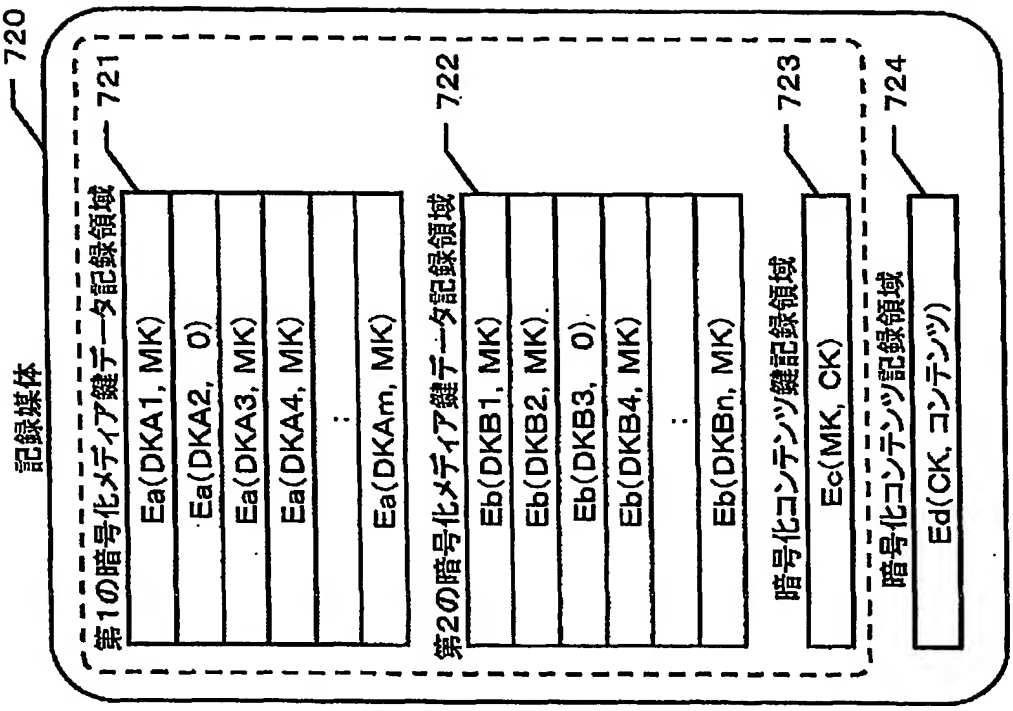

720
記録媒体
第1の暗号化メディア鍵データ記録領域
721
Ea(DKA1, MK)
Ea(DKA2, 0)
Ea(DKA3, MK)
Ea(DKA4, MK)
Ea(DKAm, MK)
第2の暗号化メディア鍵データ記録領域
722
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
暗号化コンテンツ鍵記録領域
723
Ec(MK, CK)
暗号化コンテンツ記録領域
724
Ed(CK, コンテンツ)

図13

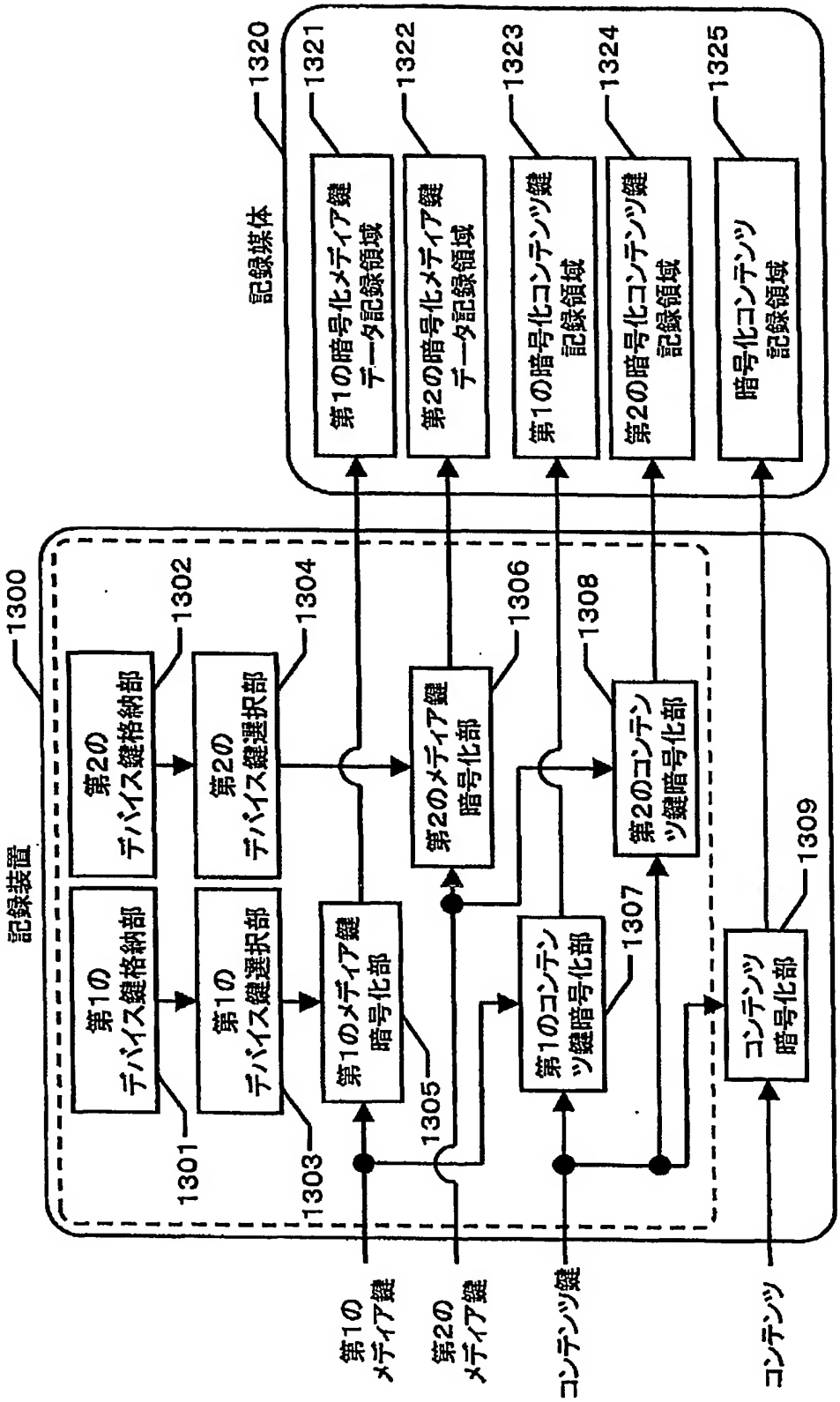

記録装置
1300
第1の
デバイス鍵格納部
1301
第2の
デバイス鍵格納部
1302
第1の
デバイス鍵選択部
1303
第2の
デバイス鍵選択部
1304
第1のメディア鍵
暗号化部
1305
第2のメディア鍵
暗号化部
1306
第1のコンテン
ツ鍵暗号化部
1307
第2のコンテン
ツ鍵暗号化部
1308
コンテンツ
暗号化部
1309
記録媒体
1320
第1の暗号化メディア鍵
データ記録領域
1321
第2の暗号化メディア鍵
データ記録領域
1322
第1の暗号化コンテンツ鍵
記録領域
1323
第2の暗号化コンテンツ鍵
記録領域
1324
暗号化コンテンツ
記録領域
1325
第1の
メディア鍵
第2の
メディア鍵
コンテンツ鍵
コンテンツ

図14

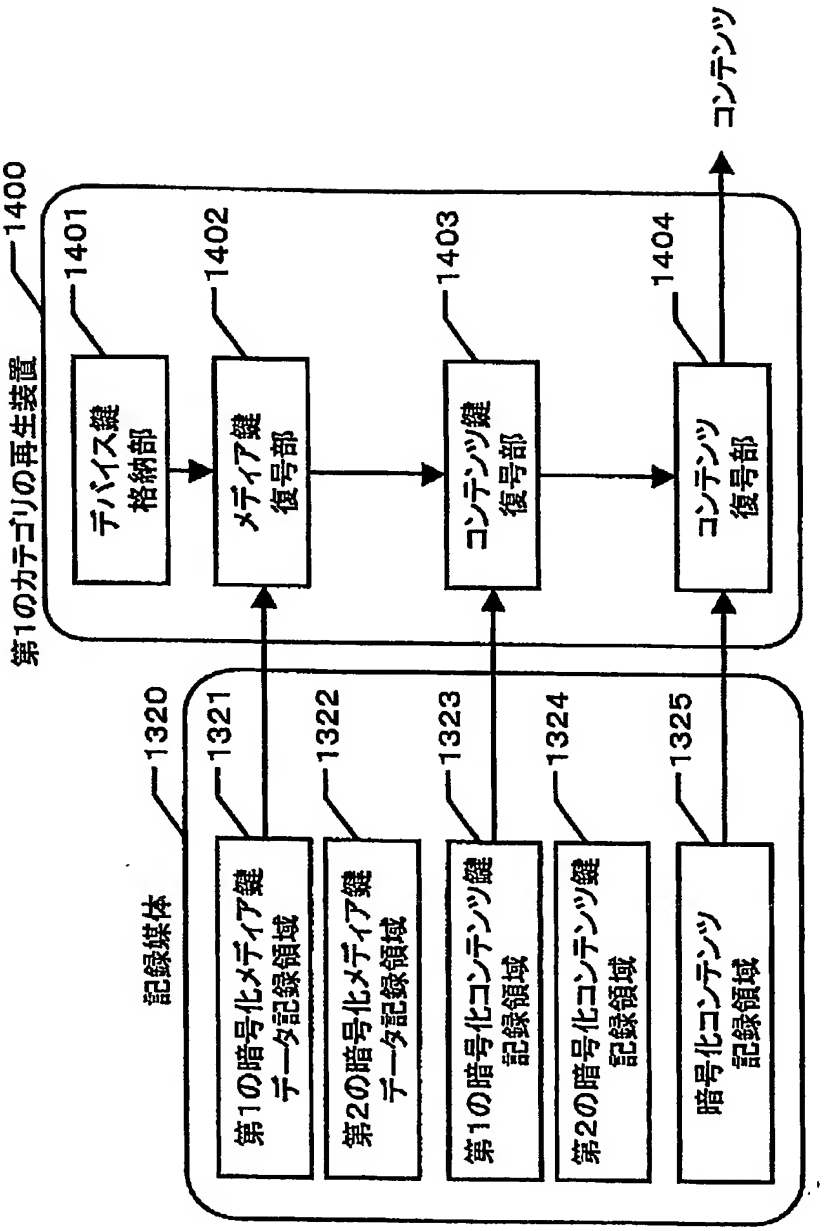

コンテンツ
第1のカテゴリの再生装置
1400
1401
デバイス鍵
格納部
1402
メディア鍵
復号部
1403
コンテンツ鍵
復号部
1404
コンテンツ
復号部
記録媒体
1320
1321
第1の暗号化メディア鍵
データ記録領域
1322
第2の暗号化メディア鍵
データ記録領域
1323
第1の暗号化コンテンツ鍵
記録領域
1324
第2の暗号化コンテンツ鍵
記録領域
1325
暗号化コンテンツ
記録領域

図15

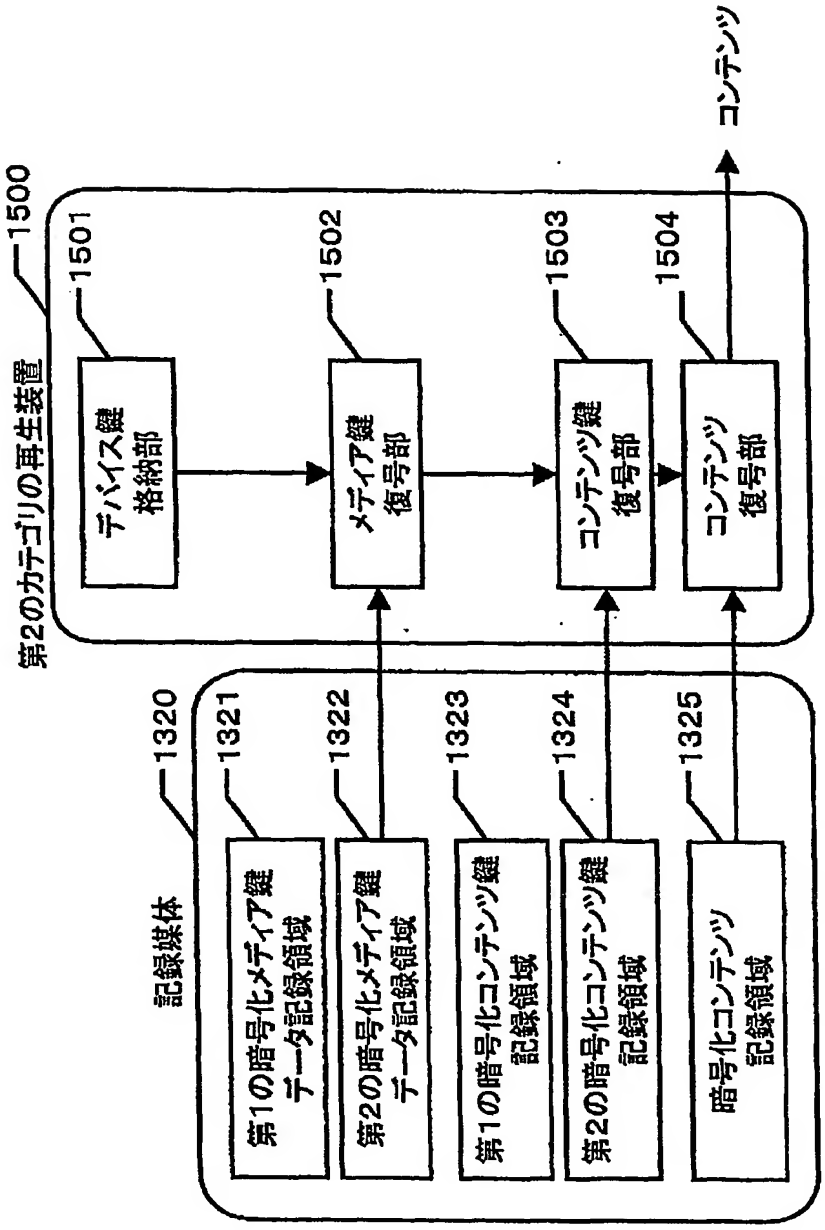

コンテンツ
1500
第2のカテゴリの再生装置
1501
デバイス鍵
格納部
1502
メディア鍵
復号部
1503
コンテンツ鍵
復号部
1504
コンテンツ
復号部
1320
記録媒体
1321
第1の暗号化メディア鍵
データ記録領域
1322
第2の暗号化メディア鍵
データ記録領域
1323
第1の暗号化コンテンツ鍵
記録領域
1324
第2の暗号化コンテンツ鍵
記録領域
1325
暗号化コンテンツ
記録領域

図16

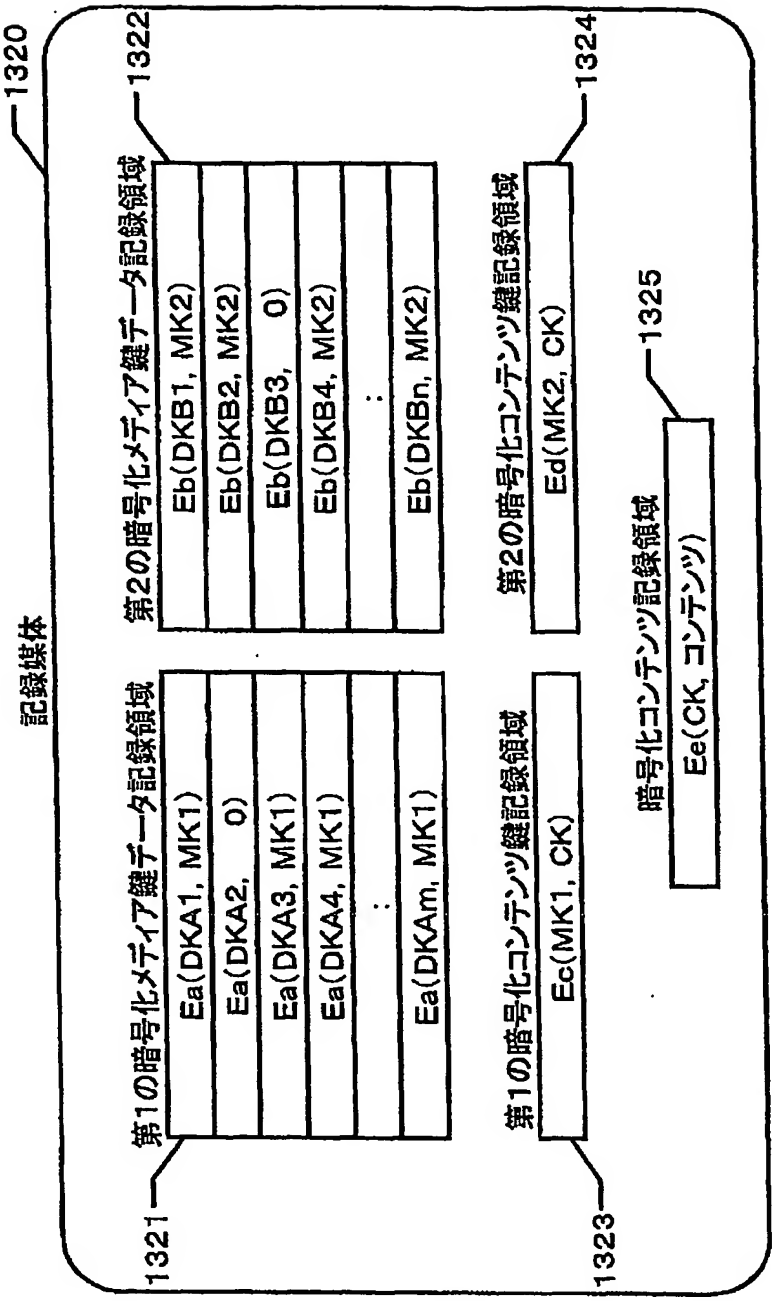

1320
記録媒体
第1の暗号化メディア鍵データ記録領域
1321
Ea(DKA1, MK1)
Ea(DKA2, 0)
Ea(DKA3, MK1)
Ea(DKA4, MK1)
Ea(DKAm, MK1)
第2の暗号化メディア鍵データ記録領域
1322
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
第1の暗号化コンテンツ鍵記録領域
1323
Ec(MK1, CK)
第2の暗号化コンテンツ鍵記録領域
1324
Ed(MK2, CK)
暗号化コンテンツ記録領域
1325
Ee(CK, コンテンツ)

図17

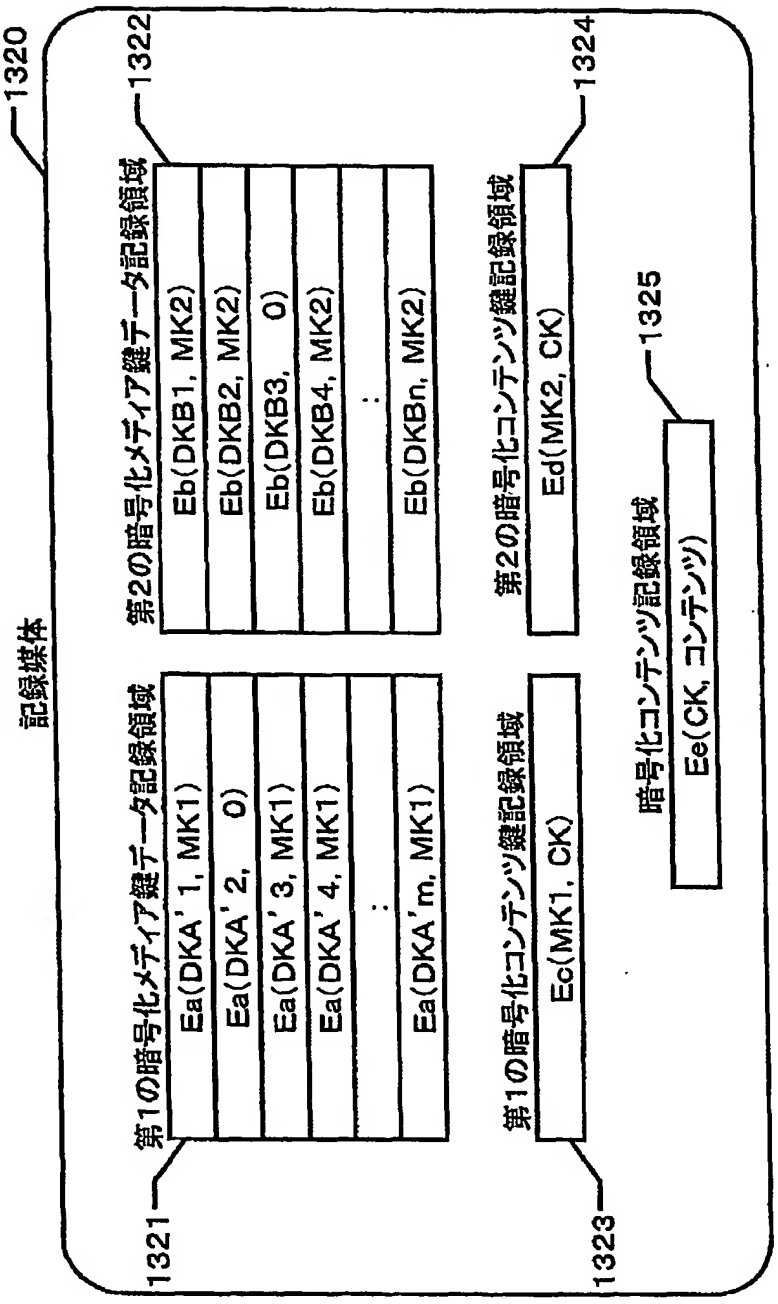

1320
記録媒体
第1の暗号化メディア鍵データ記録領域
Ea(DKA'1, MK1)
Ea(DKA'2, 0)
Ea(DKA'3, MK1)
Ea(DKA'4, MK1)
Ea(DKA'm, MK1)
1321
第2の暗号化メディア鍵データ記録領域
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
1322
第1の暗号化コンテンツ鍵記録領域
Ec(MK1, CK)
1323
第2の暗号化コンテンツ鍵記録領域
Ed(MK2, CK)
1324
暗号化コンテンツ記録領域
Ee(CK, コンテンツ)
1325

図18

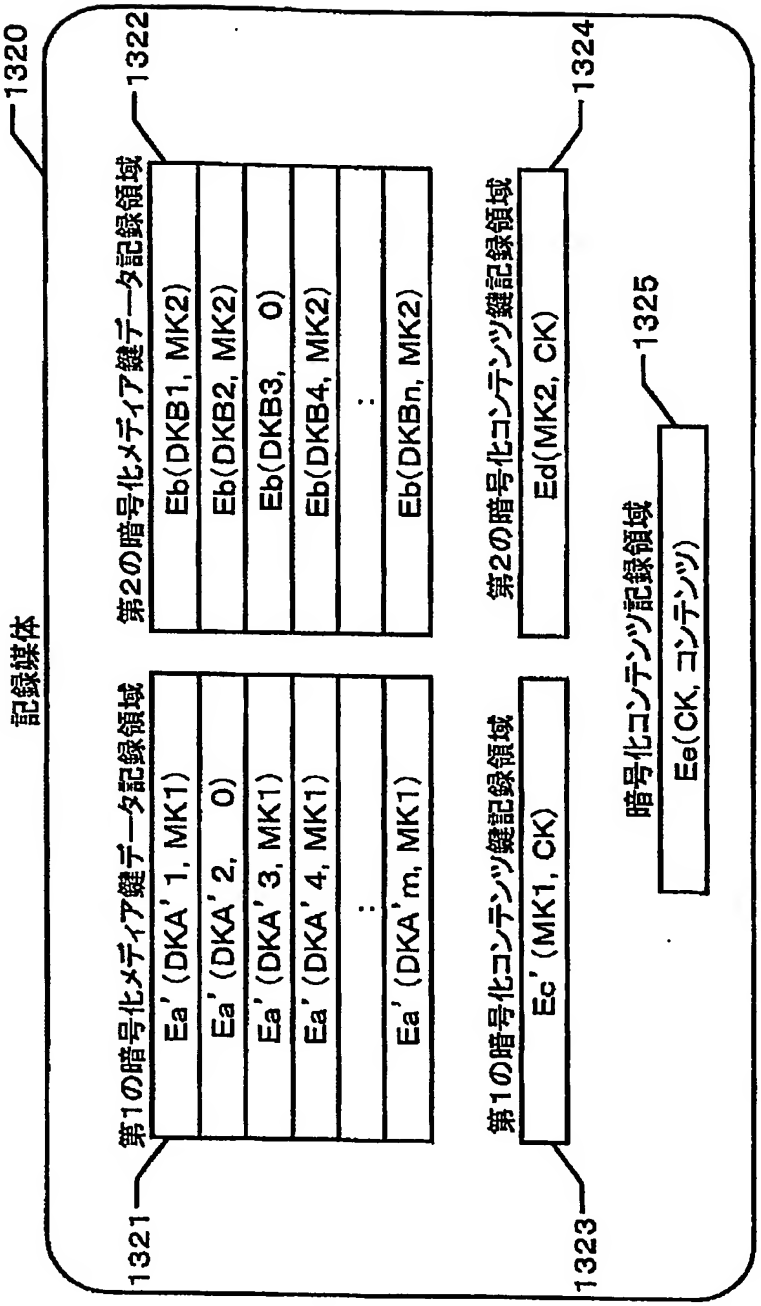

記録媒体
1320
第1の暗号化メディア鍵データ記録領域
1321
Ea'(DKA'1, MK1)
Ea'(DKA'2, 0)
Ea'(DKA'3, MK1)
Ea'(DKA'4, MK1)
Ea'(DKA'm, MK1)
第2の暗号化メディア鍵データ記録領域
1322
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
第1の暗号化コンテンツ鍵記録領域
1323
Ec'(MK1, CK)
第2の暗号化コンテンツ鍵記録領域
1324
Ed(MK2, CK)
暗号化コンテンツ記録領域
1325
Ee(CK, コンテンツ)

図19

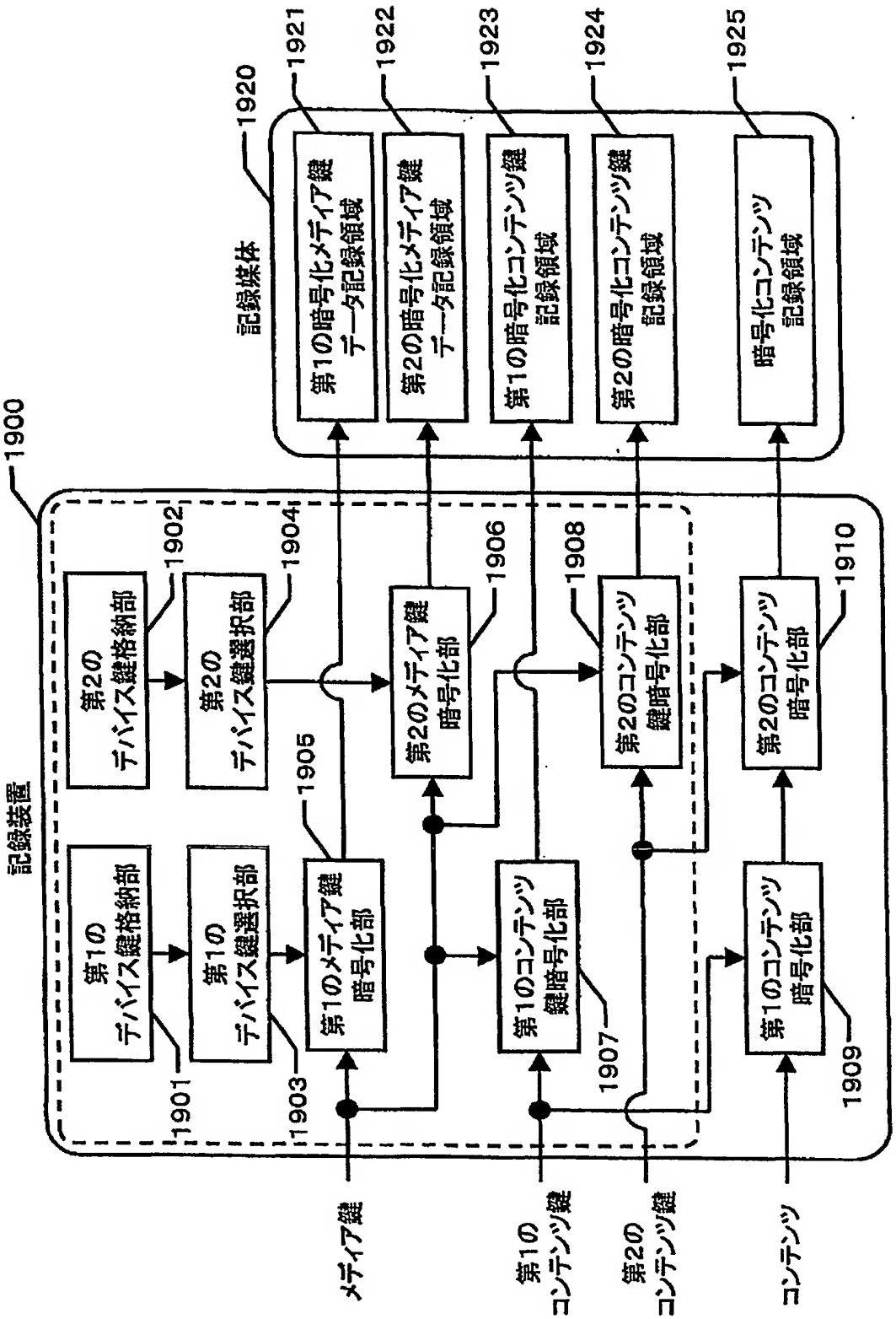

1900
記録装置
記録媒体
1920
1921
1922
1923
1924
1925
第1の暗号化メディア鍵 データ記録領域
第2の暗号化メディア鍵 データ記録領域
第1の暗号化コンテンツ鍵 記録領域
第2の暗号化コンテンツ鍵 記録領域
暗号化コンテンツ 記録領域
第1の デバイス鍵格納部
第2の デバイス鍵格納部
第1の デバイス鍵選択部
第2の デバイス鍵選択部
第1のメディア鍵 暗号化部
第2のメディア鍵 暗号化部
第1のコンテンツ 鍵暗号化部
第2のコンテンツ 鍵暗号化部
第1のコンテンツ 暗号化部
第2のコンテンツ 暗号化部
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
メディア鍵
第1の コンテンツ鍵
第2の コンテンツ鍵
コンテンツ

図20

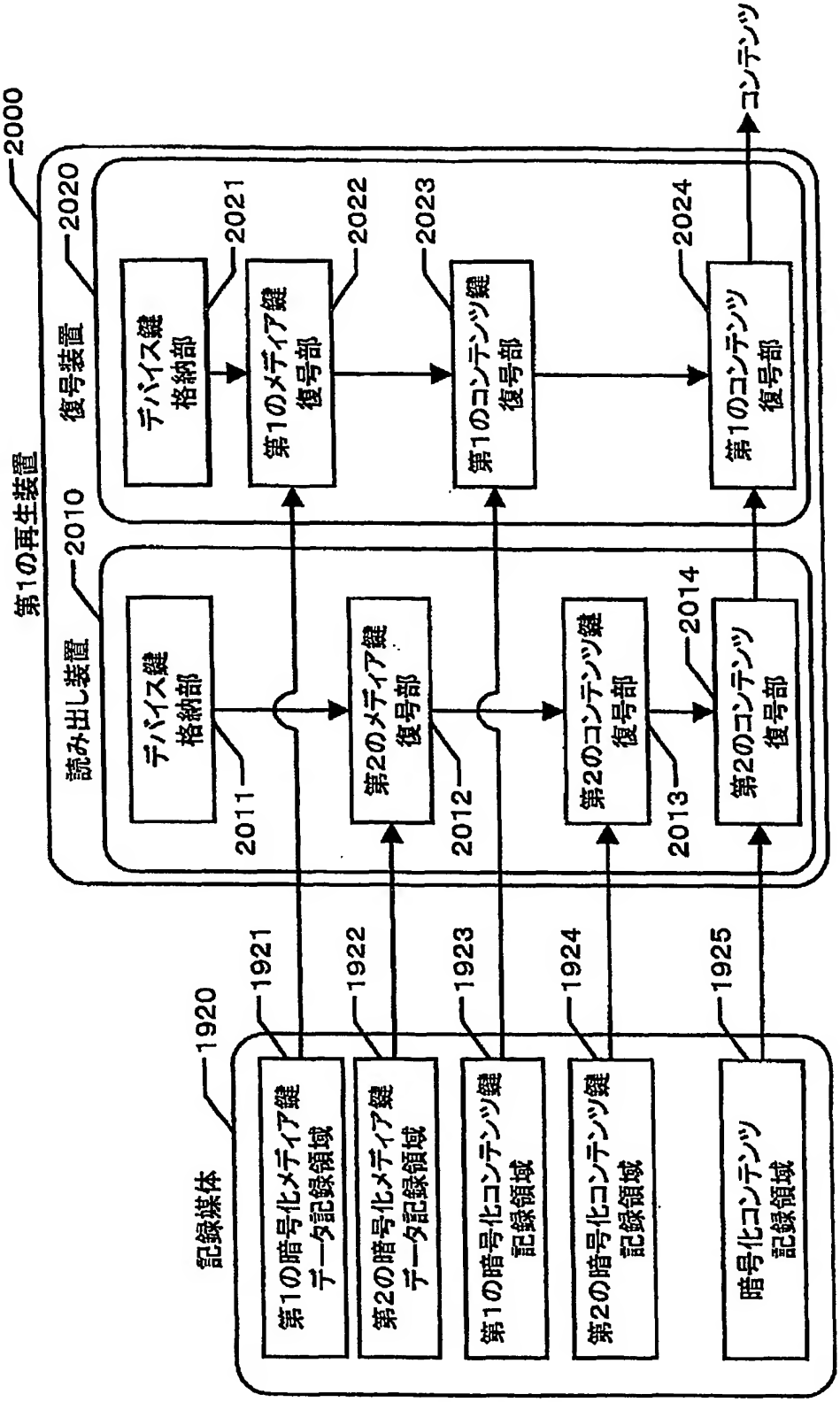

2000
第1の再生装置
2010
読み出し装置
2020
復号装置
デバイス鍵格納部
2011
第2のメディア鍵復号部
2012
第2のコンテンツ鍵復号部
2013
第2のコンテンツ復号部
2014
2021
デバイス鍵格納部
2022
第1のメディア鍵復号部
2023
第1のコンテンツ鍵復号部
2024
第1のコンテンツ復号部
コンテンツ
1920
記録媒体
1921
第1の暗号化メディア鍵データ記録領域
1922
第2の暗号化メディア鍵データ記録領域
1923
第1の暗号化コンテンツ鍵記録領域
1924
第2の暗号化コンテンツ鍵記録領域
1925
暗号化コンテンツ記録領域

図21

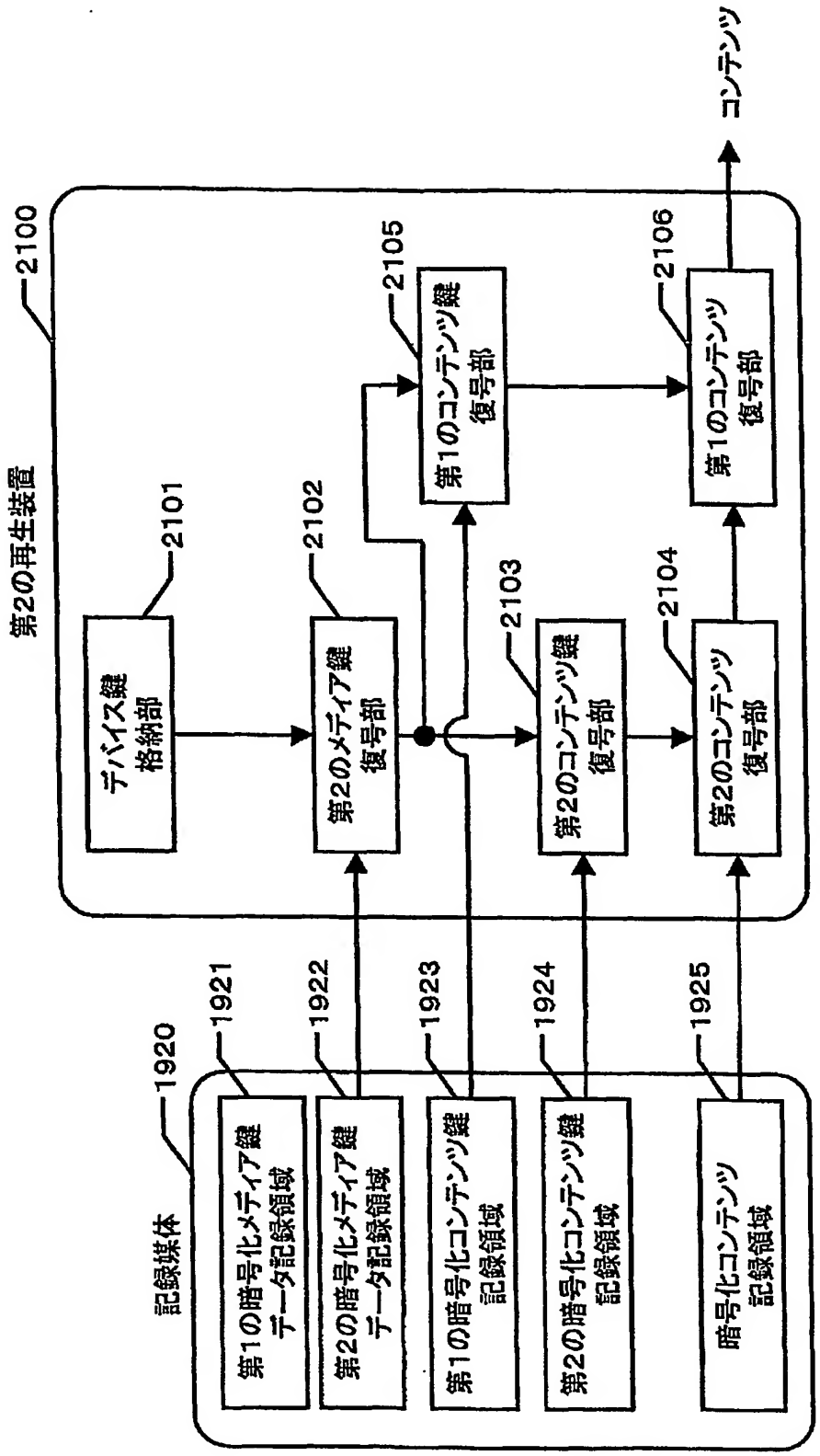

コンテンツ
2100
第2の再生装置
2101
デバイス鍵
格納部
2102
第2のメディア鍵
復号部
2103
第2のコンテンツ鍵
復号部
2104
第2のコンテンツ
復号部
2105
第1のコンテンツ鍵
復号部
2106
第1のコンテンツ
復号部
1920
記録媒体
1921
第1の暗号化メディア鍵
データ記録領域
1922
第2の暗号化メディア鍵
データ記録領域
1923
第1の暗号化コンテンツ鍵
記録領域
1924
第2の暗号化コンテンツ鍵
記録領域
1925
暗号化コンテンツ
記録領域

図22

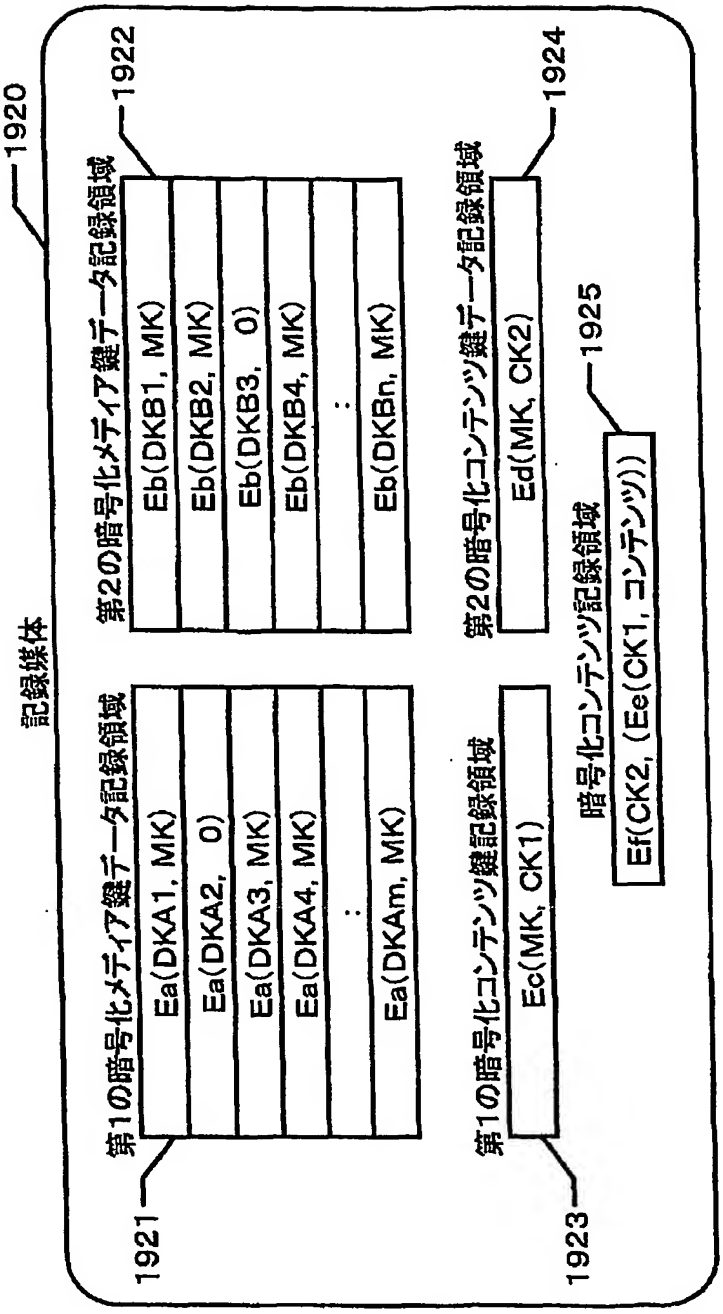

1920
記録媒体
第1の暗号化メディア鍵データ記録領域
Ea(DKA1, MK)
Ea(DKA2, 0)
Ea(DKA3, MK)
Ea(DKA4, MK)
Ea(DKAm, MK)
1921
第2の暗号化メディア鍵データ記録領域
1922
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
第1の暗号化コンテンツ鍵記録領域
Ec(MK, CK1)
1923
第2の暗号化コンテンツ鍵データ記録領域
1924
Ed(MK, CK2)
暗号化コンテンツ記録領域
1925
Ef(CK2, (Ee(CK1, コンテンツ))

図23

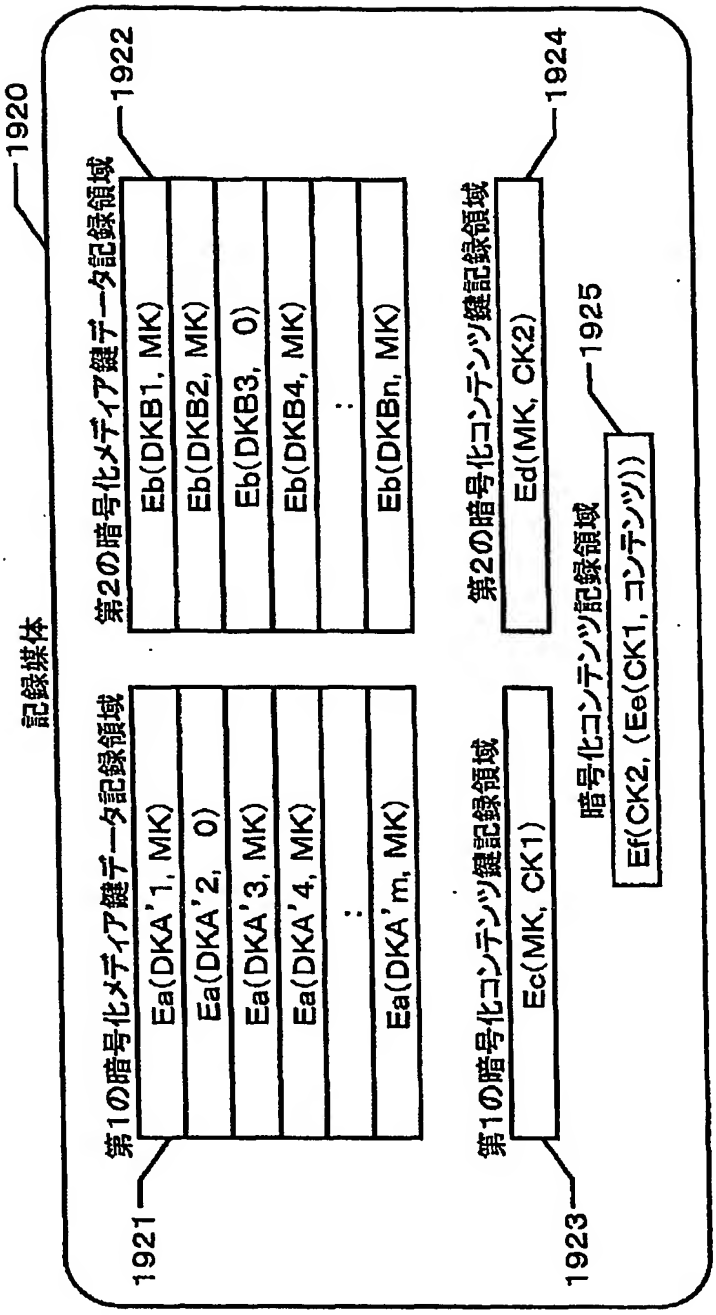

1920
記録媒体
第2の暗号化メディア鍵データ記録領域
1922
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
第2の暗号化コンテンツ鍵記録領域
1924
Ed(MK, CK2)
暗号化コンテンツ記録領域
1925
Ef(CK2, (Ee(CK1, コンテンツ)))
第1の暗号化メディア鍵データ記録領域
Ea(DKA'1, MK)
Ea(DKA'2, 0)
Ea(DKA'3, MK)
Ea(DKA'4, MK)
Ea(DKA'm, MK)
1921
第1の暗号化コンテンツ鍵記録領域
Ec(MK, CK1)
1923

図24

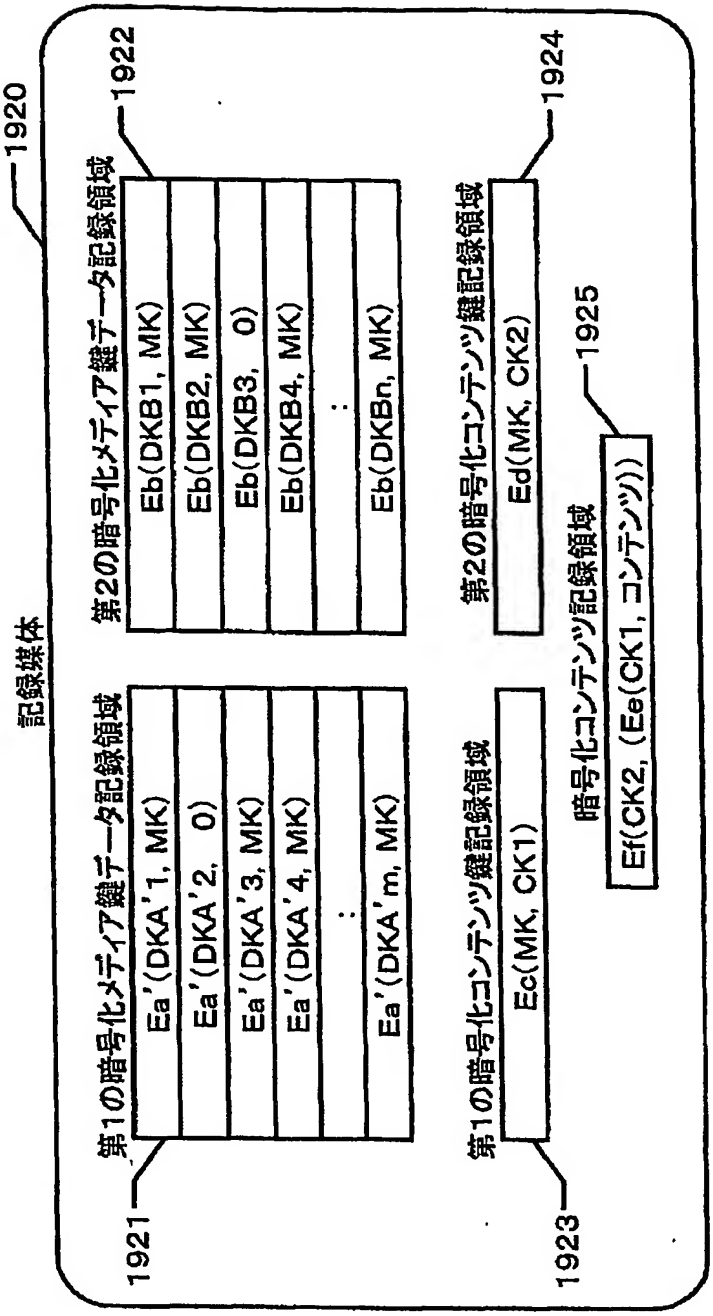

1920
記録媒体
第2の暗号化メディア鍵データ記録領域
1922
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
第2の暗号化コンテンツ鍵記録領域
1924
Ed(MK, CK2)
暗号化コンテンツ記録領域
1925
Ef(CK2, (Ee(CK1, コンテンツ)))
第1の暗号化メディア鍵データ記録領域
Ea'(DKA'1, MK)
Ea'(DKA'2, 0)
Ea'(DKA'3, MK)
Ea'(DKA'4, MK)
Ea'(DKA'm, MK)
1921
第1の暗号化コンテンツ鍵記録領域
Ec(MK, CK1)
1923

図25

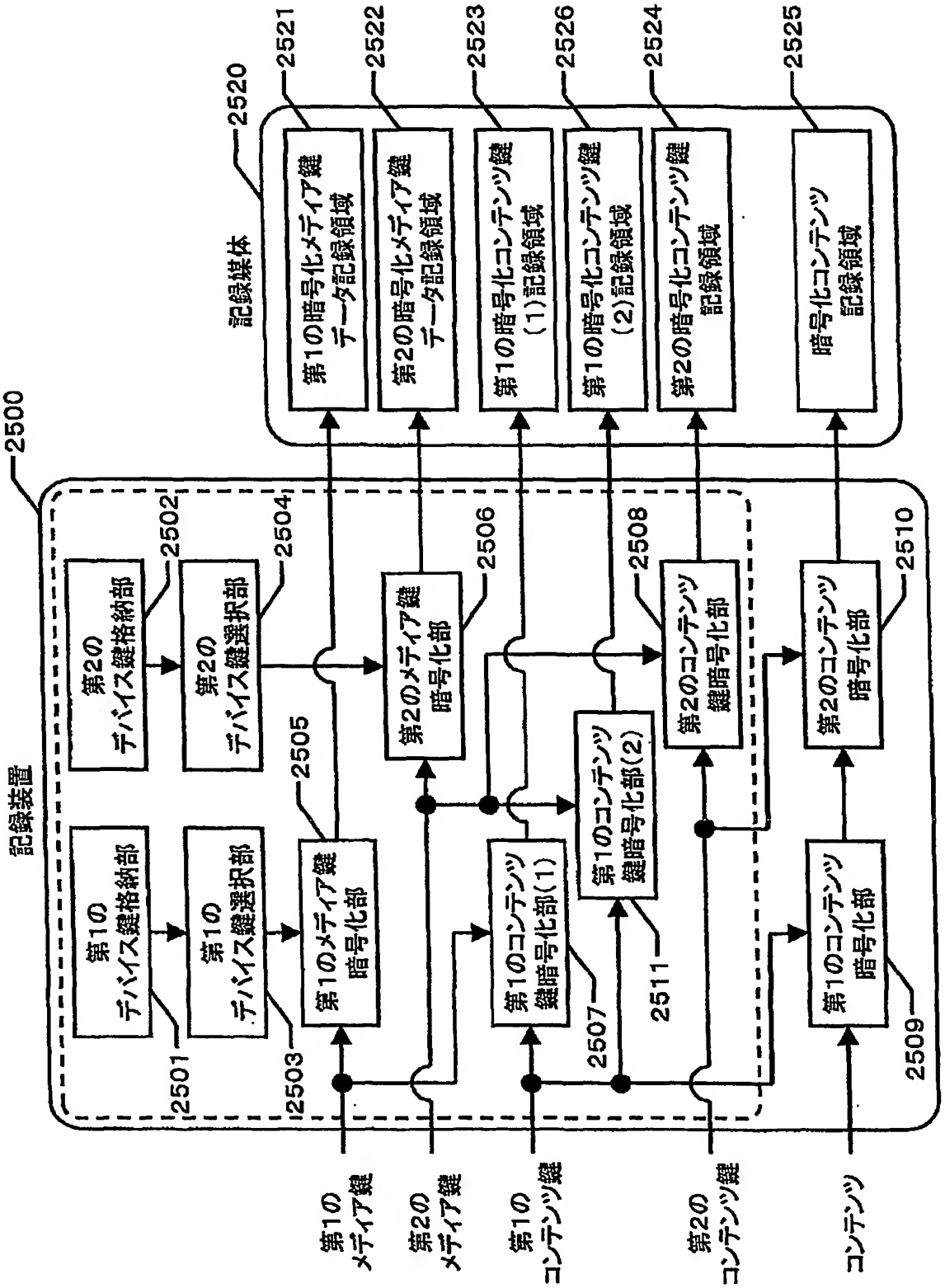

2500
記録装置
2501
2502
第2の
デバイス鍵格納部
2503
第1の
デバイス鍵格納部
2504
第2の
デバイス鍵選択部
2505
第1の
デバイス鍵選択部
2506
第1のメディア鍵
暗号化部
2507
第2のメディア鍵
暗号化部
2508
第1のコンテンツ
鍵暗号化部(1)
2509
第1のコンテンツ
鍵暗号化部(2)
2510
第2のコンテンツ
鍵暗号化部
2511
第1のコンテンツ
暗号化部
第2のコンテンツ
暗号化部
2520
記録媒体
2521
第1の暗号化メディア鍵
データ記録領域
2522
第2の暗号化メディア鍵
データ記録領域
2523
第1の暗号化コンテンツ鍵
(1)記録領域
2526
第1の暗号化コンテンツ鍵
(2)記録領域
2524
第2の暗号化コンテンツ鍵
記録領域
2525
暗号化コンテンツ
記録領域
第1の
メディア鍵
第2の
メディア鍵
第1の
コンテンツ鍵
第2の
コンテンツ鍵
コンテンツ

図26

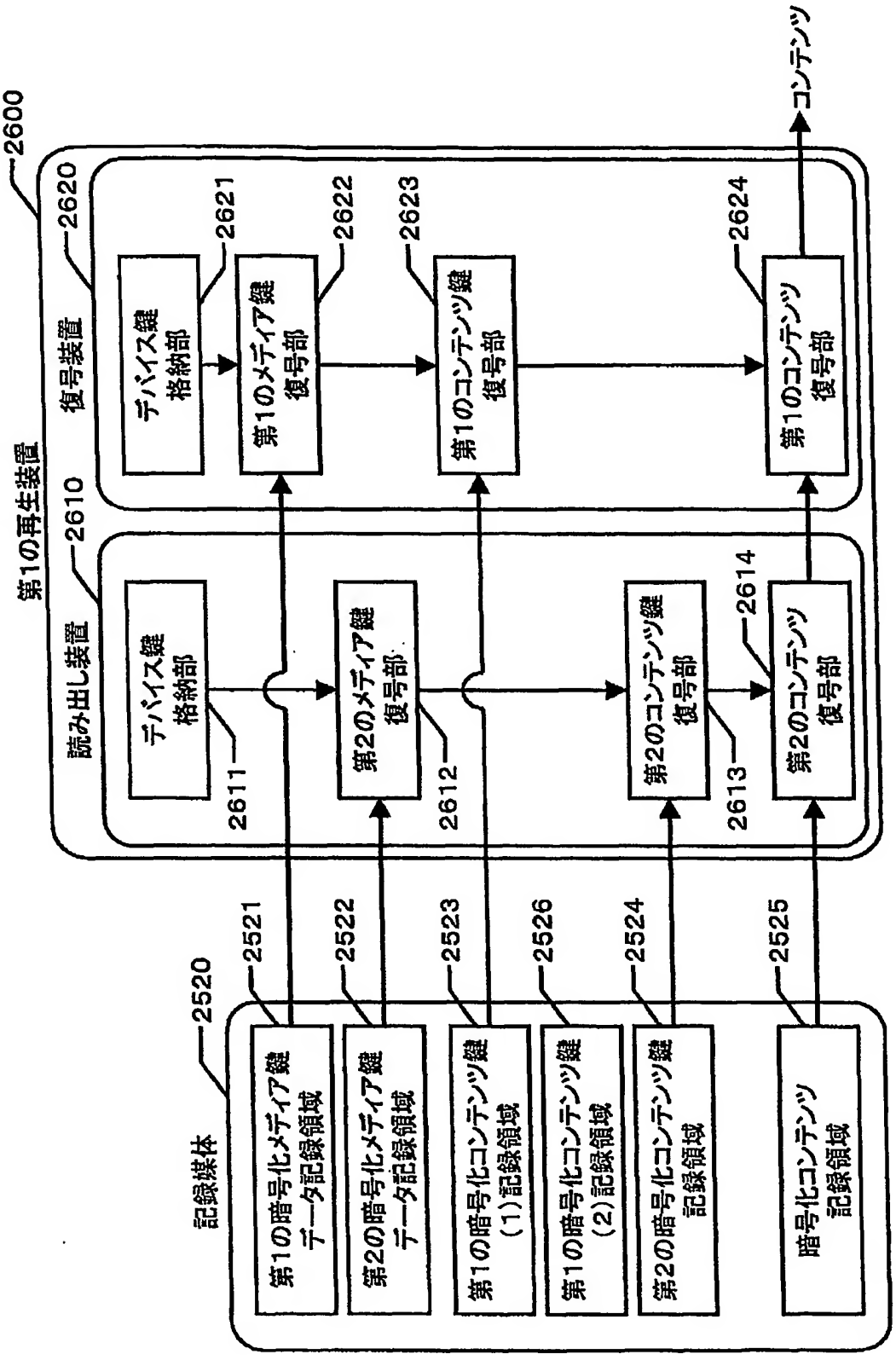

2600
第1の再生装置
2610
読み出し装置
2611
デバイス鍵格納部
2612
第2のメディア鍵復号部
2613
第2のコンテンツ鍵復号部
2614
第2のコンテンツ復号部
2620
復号装置
2621
デバイス鍵格納部
2622
第1のメディア鍵復号部
2623
第1のコンテンツ鍵復号部
2624
第1のコンテンツ復号部
コンテンツ
2520
記録媒体
2521
第1の暗号化メディア鍵データ記録領域
2522
第2の暗号化メディア鍵データ記録領域
2523
第1の暗号化コンテンツ鍵(1)記録領域
2526
第1の暗号化コンテンツ鍵(2)記録領域
2524
第2の暗号化コンテンツ鍵記録領域
2525
暗号化コンテンツ記録領域

図27

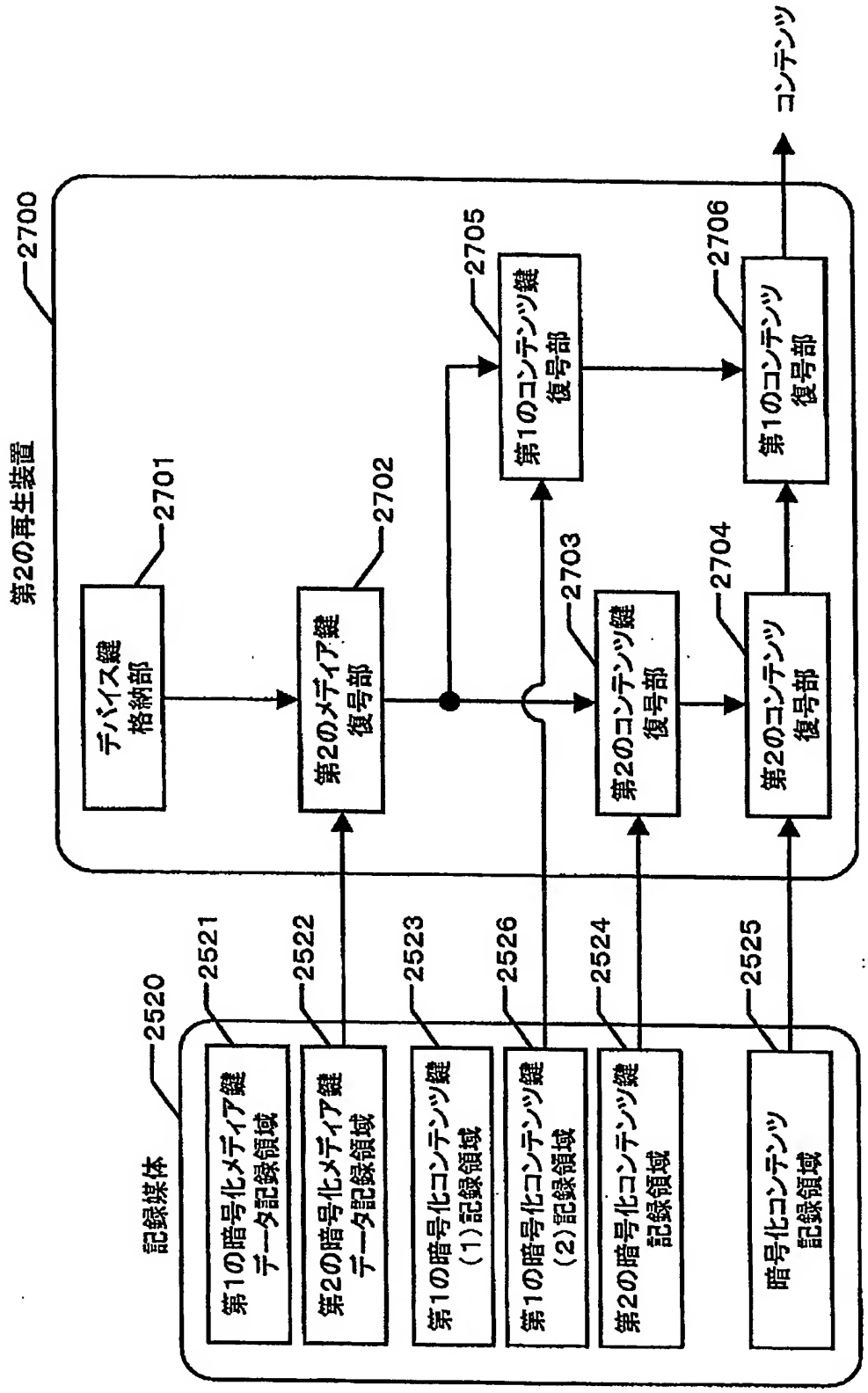

コンテンツ
2700
第2の再生装置
2701
デバイス鍵
格納部
2702
第2のメディア鍵
復号部
2703
第2のコンテンツ鍵
復号部
2704
第2のコンテンツ
復号部
2705
第1のコンテンツ鍵
復号部
2706
第1のコンテンツ
復号部
2520
記録媒体
2521
第1の暗号化メディア鍵
データ記録領域
2522
第2の暗号化メディア鍵
データ記録領域
2523
第1の暗号化コンテンツ鍵
(1)記録領域
2526
第1の暗号化コンテンツ鍵
(2)記録領域
2524
第2の暗号化コンテンツ鍵
記録領域
2525
暗号化コンテンツ
記録領域

図28

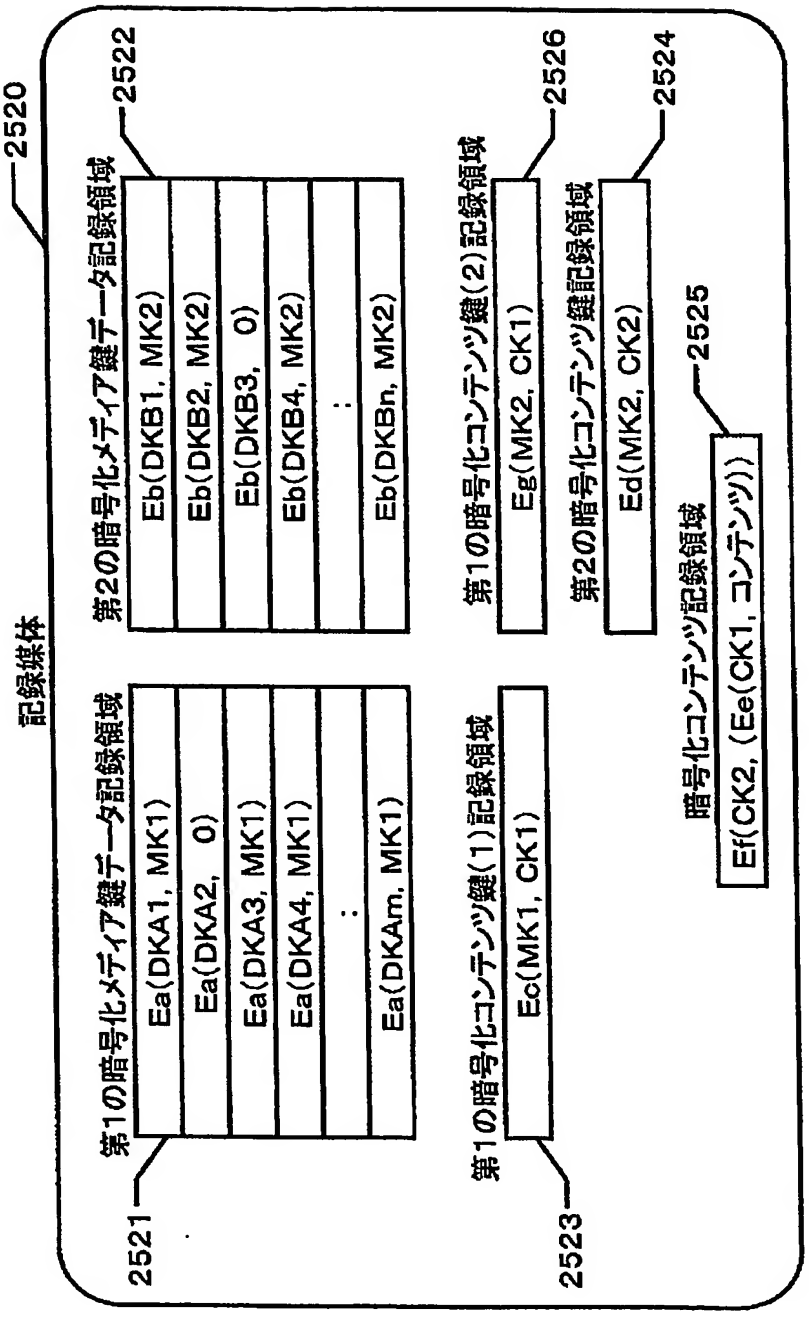

2520
記録媒体
第2の暗号化メディア鍵データ記録領域
2522
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
第1の暗号化コンテンツ鍵(2)記録領域
2526
Eg(MK2, CK1)
第2の暗号化コンテンツ鍵記録領域
2524
Ed(MK2, CK2)
暗号化コンテンツ記録領域
2525
Ef(CK2, (Ee(CK1, コンテンツ))
第1の暗号化メディア鍵データ記録領域
Ea(DKA1, MK1)
Ea(DKA2, 0)
Ea(DKA3, MK1)
Ea(DKA4, MK1)
Ea(DKAm, MK1)
2521
第1の暗号化コンテンツ鍵(1)記録領域
Ec(MK1, CK1)
2523

図29

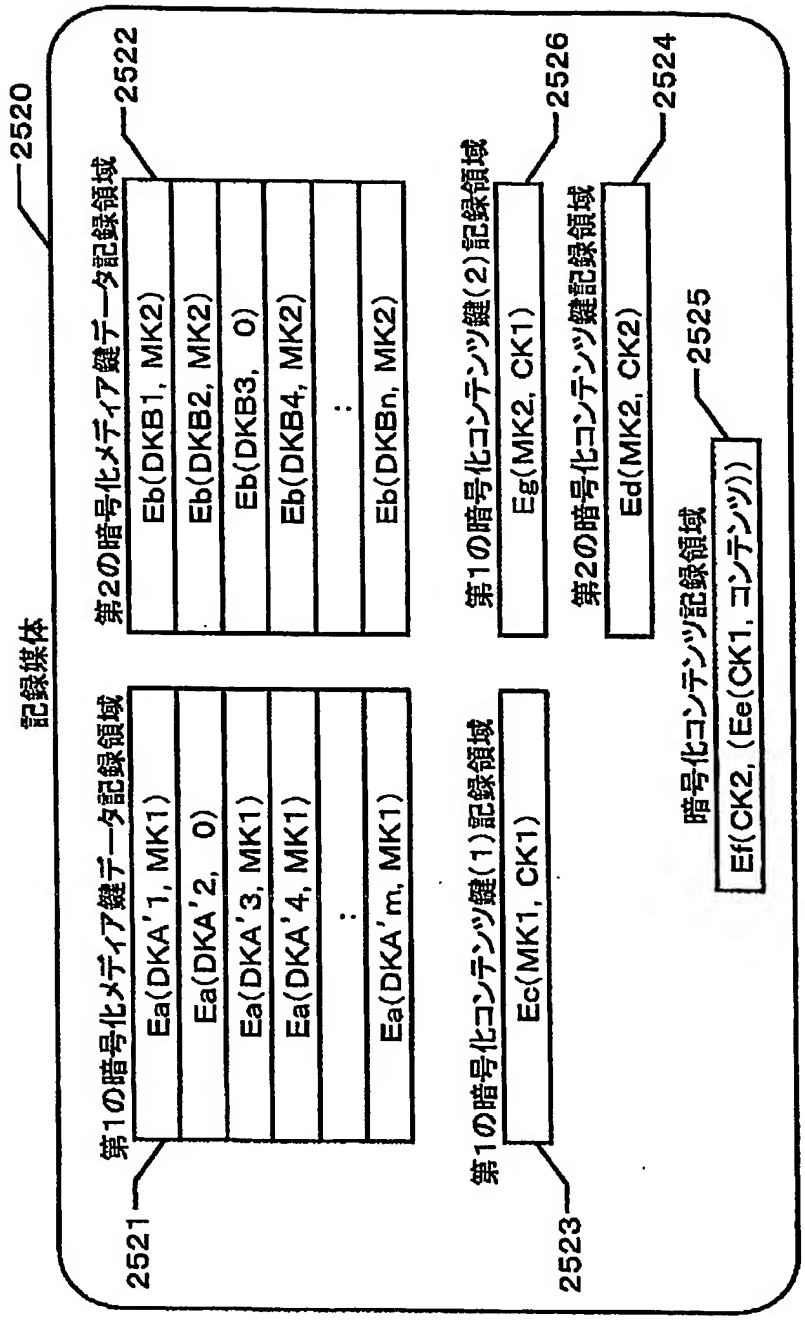

2520
記録媒体
第1の暗号化メディア鍵データ記録領域
2521
Ea(DKA'1, MK1)
Ea(DKA'2, 0)
Ea(DKA'3, MK1)
Ea(DKA'4, MK1)
Ea(DKA'm, MK1)
第2の暗号化メディア鍵データ記録領域
2522
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
第1の暗号化コンテンツ鍵(1)記録領域
2523
Ec(MK1, CK1)
第1の暗号化コンテンツ鍵(2)記録領域
2526
Eg(MK2, CK1)
第2の暗号化コンテンツ鍵記録領域
2524
Ed(MK2, CK2)
暗号化コンテンツ記録領域
2525
Ef(CK2, (Ee(CK1, コンテンツ)))

図30

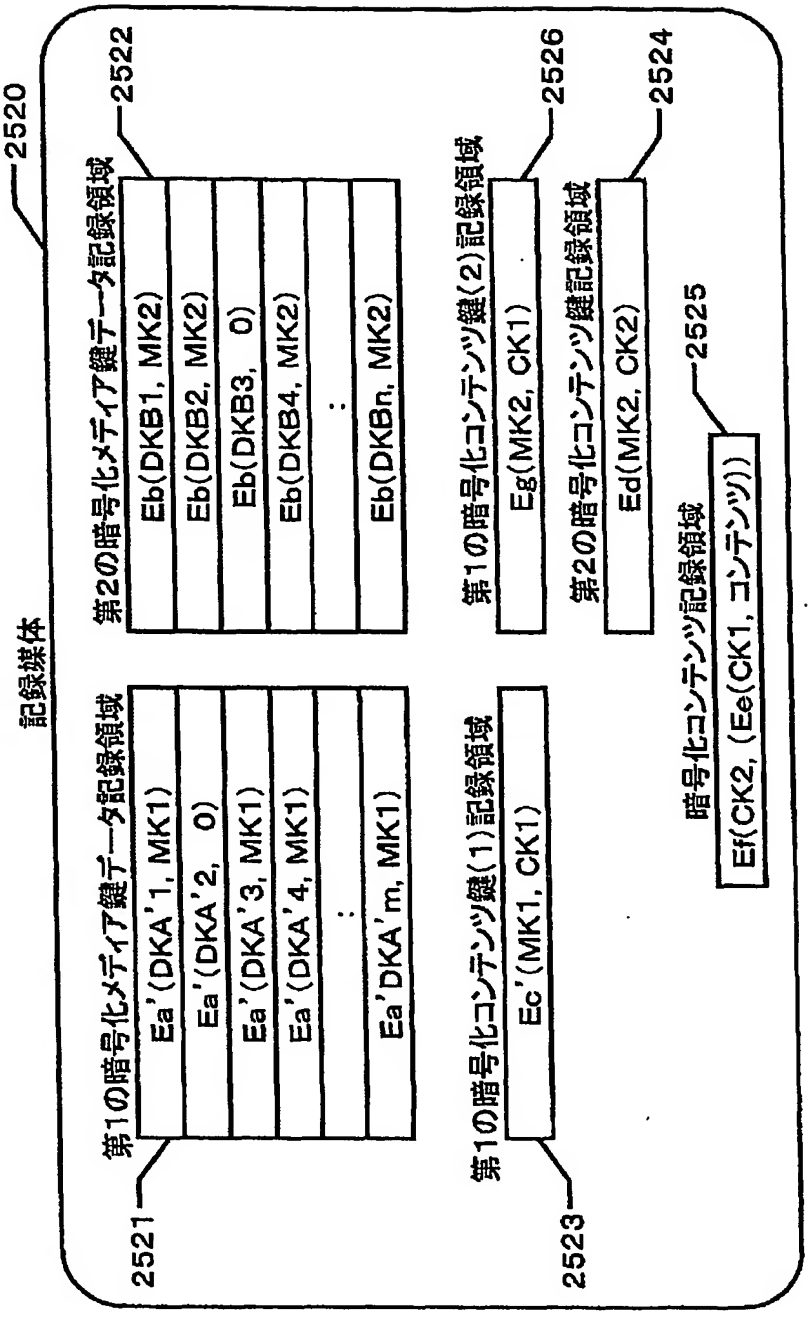

2520
記録媒体
第2の暗号化メディア鍵データ記録領域
2522
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
第1の暗号化メディア鍵データ記録領域
Ea'(DKA'1, MK1)
Ea'(DKA'2, 0)
Ea'(DKA'3, MK1)
Ea'(DKA'4, MK1)
Ea'DKA'm, MK1)
2521
第1の暗号化コンテンツ鍵(1)記録領域
Ec'(MK1, CK1)
2523
第1の暗号化コンテンツ鍵(2)記録領域
2526
Eg(MK2, CK1)
第2の暗号化コンテンツ鍵記録領域
2524
Ed(MK2, CK2)
暗号化コンテンツ記録領域
2525
Ef(CK2, (Ee(CK1, コンテンツ))

図31

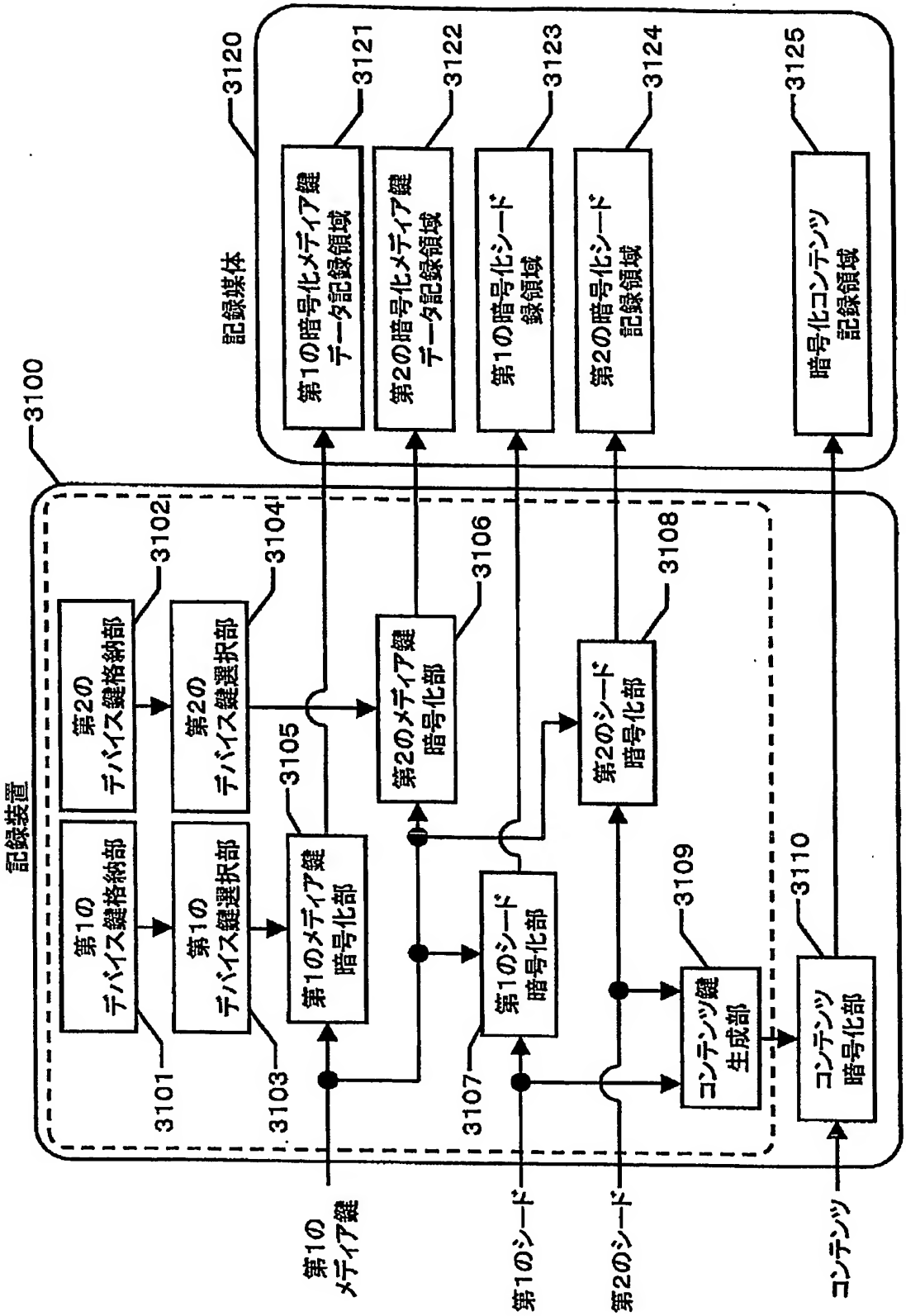

3100
記録装置
記録媒体
3120
3121
3122
3123
3124
3125
第1の暗号化メディア鍵データ記録領域
第2の暗号化メディア鍵データ記録領域
第1の暗号化シード録領域
第2の暗号化シード記録領域
暗号化コンテンツ記録領域
第1のデバイス鍵格納部
第2のデバイス鍵格納部
第1のデバイス鍵選択部
第2のデバイス鍵選択部
第1のメディア鍵暗号化部
第2のメディア鍵暗号化部
第1のシード暗号化部
第2のシード暗号化部
コンテンツ鍵生成部
コンテンツ暗号化部
3101
3102
3103
3104
3105
3106
3107
3108
3109
3110
第1のメディア鍵
第1のシード
第2のシード
コンテンツ

図32

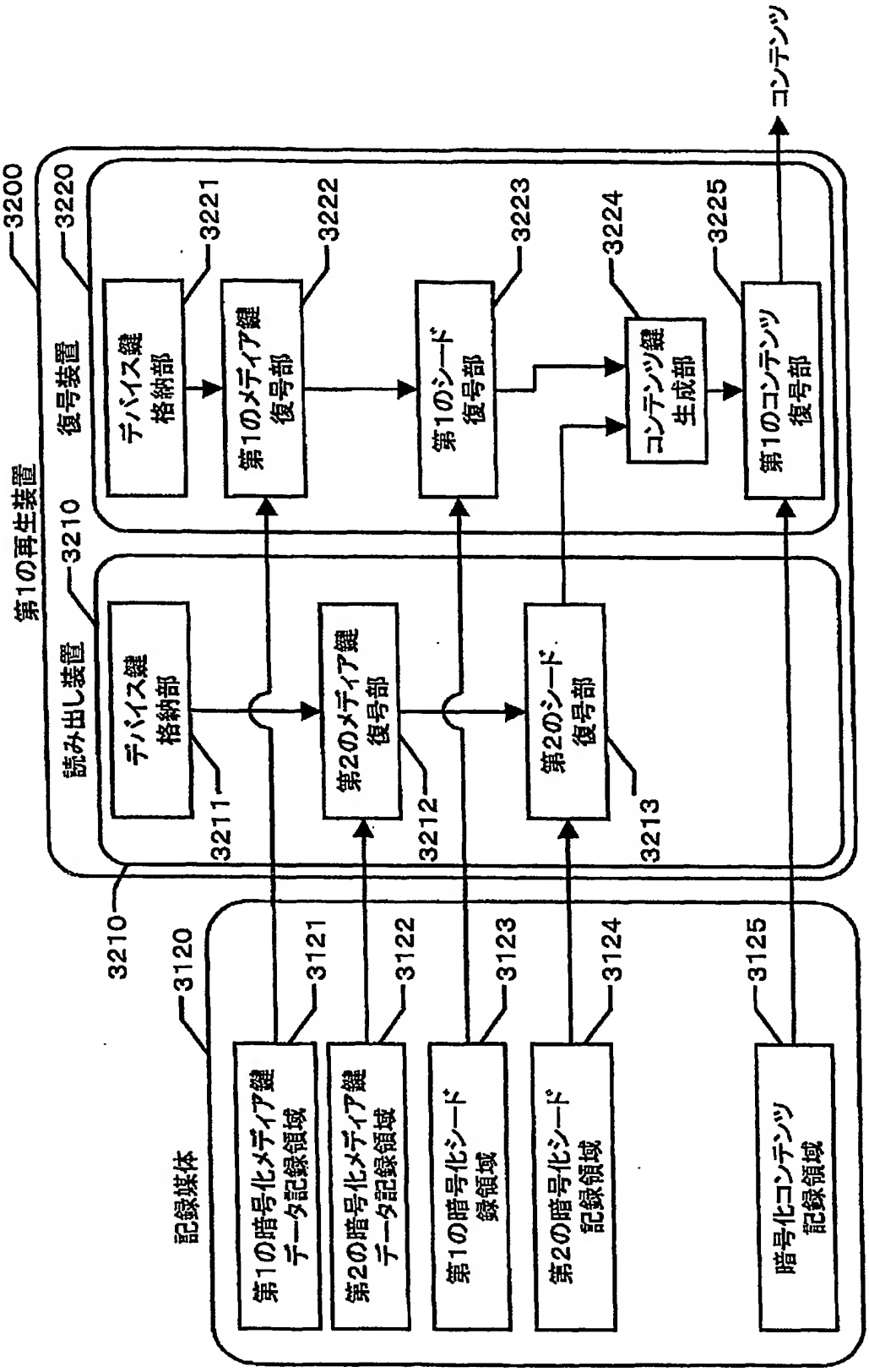

コンテンツ
3200
第1の再生装置
3220
復号装置
3221
デバイス鍵格納部
3222
第1のメディア鍵復号部
3223
第1のシード復号部
3224
コンテンツ鍵生成部
3225
第1のコンテンツ復号部
3210
読み出し装置
3211
デバイス鍵格納部
3212
第2のメディア鍵復号部
3213
第2のシード復号部
3210
3120
記録媒体
3121
第1の暗号化メディア鍵データ記録領域
3122
第2の暗号化メディア鍵データ記録領域
3123
第1の暗号化シード鍵領域
3124
第2の暗号化シード記録領域
3125
暗号化コンテンツ記録領域

図33

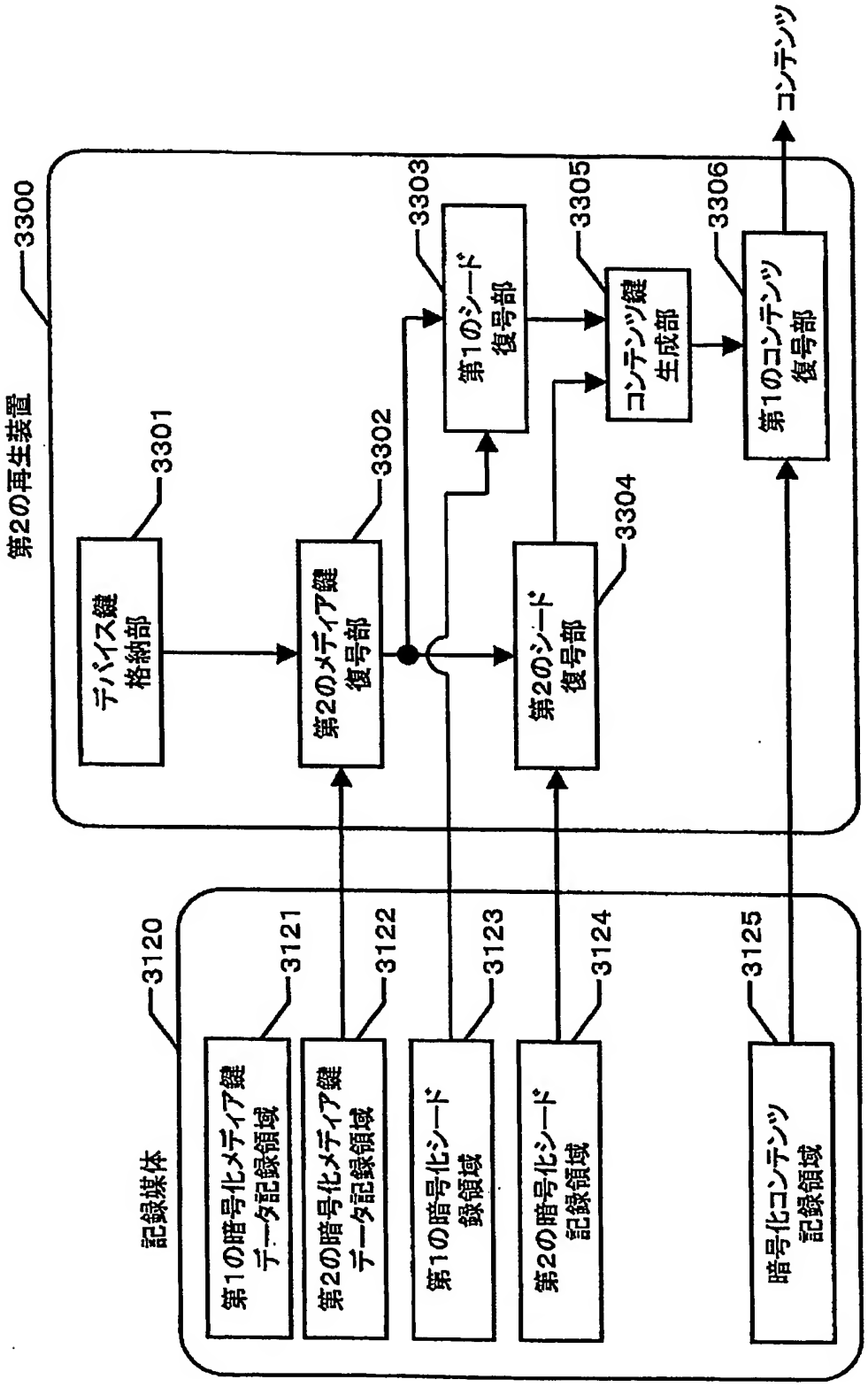

第2の再生装置
3300
デバイス鍵格納部
3301
第2のメディア鍵復号部
3302
第1のシード復号部
3303
第2のシード復号部
3304
コンテンツ鍵生成部
3305
第1のコンテンツ復号部
3306
コンテンツ
記録媒体
3120
第1の暗号化メディア鍵データ記録領域
3121
第2の暗号化メディア鍵データ記録領域
3122
第1の暗号化シード録領域
3123
第2の暗号化シード記録領域
3124
暗号化コンテンツ記録領域
3125

図34

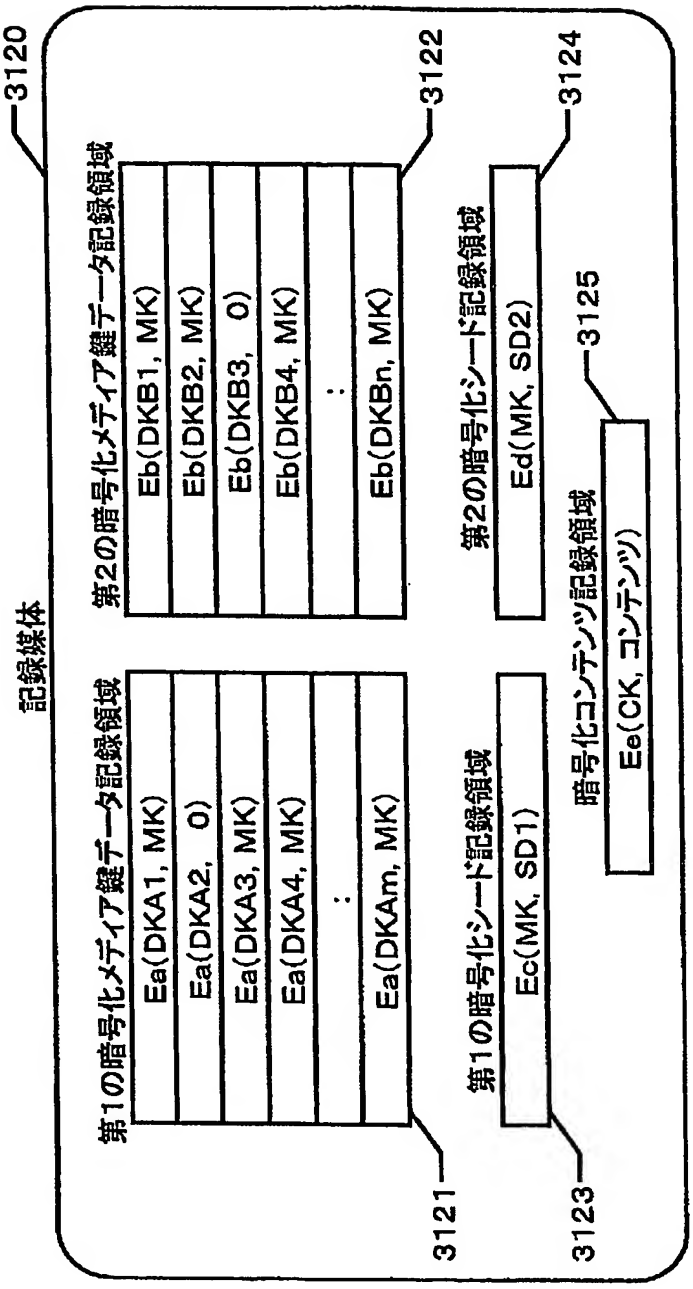

3120
記録媒体
第1の暗号化メディア鍵データ記録領域
Ea(DKA1, MK)
Ea(DKA2, 0)
Ea(DKA3, MK)
Ea(DKA4, MK)
Ea(DKAm, MK)
3121
第2の暗号化メディア鍵データ記録領域
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
3122
第1の暗号化シード記録領域
Ec(MK, SD1)
3123
第2の暗号化シード記録領域
Ed(MK, SD2)
3124
暗号化コンテンツ記録領域
Ee(CK, コンテンツ)
3125

図35

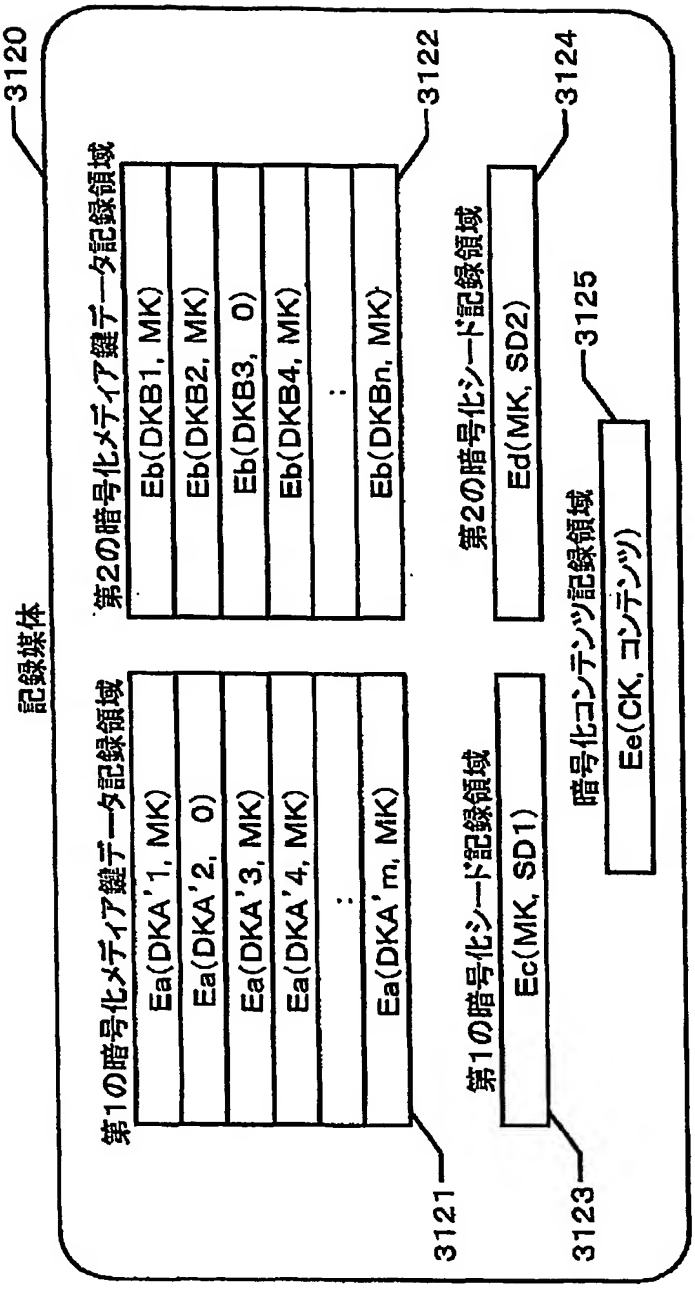

3120
記録媒体
第1の暗号化メディア鍵データ記録領域
Ea(DKA'1, MK)
Ea(DKA'2, 0)
Ea(DKA'3, MK)
Ea(DKA'4, MK)
Ea(DKA'm, MK)
3121
第2の暗号化メディア鍵データ記録領域
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
3122
第1の暗号化シード記録領域
Ec(MK, SD1)
3123
第2の暗号化シード記録領域
Ed(MK, SD2)
3124
暗号化コンテンツ記録領域
Ee(CK, コンテンツ)
3125

図36

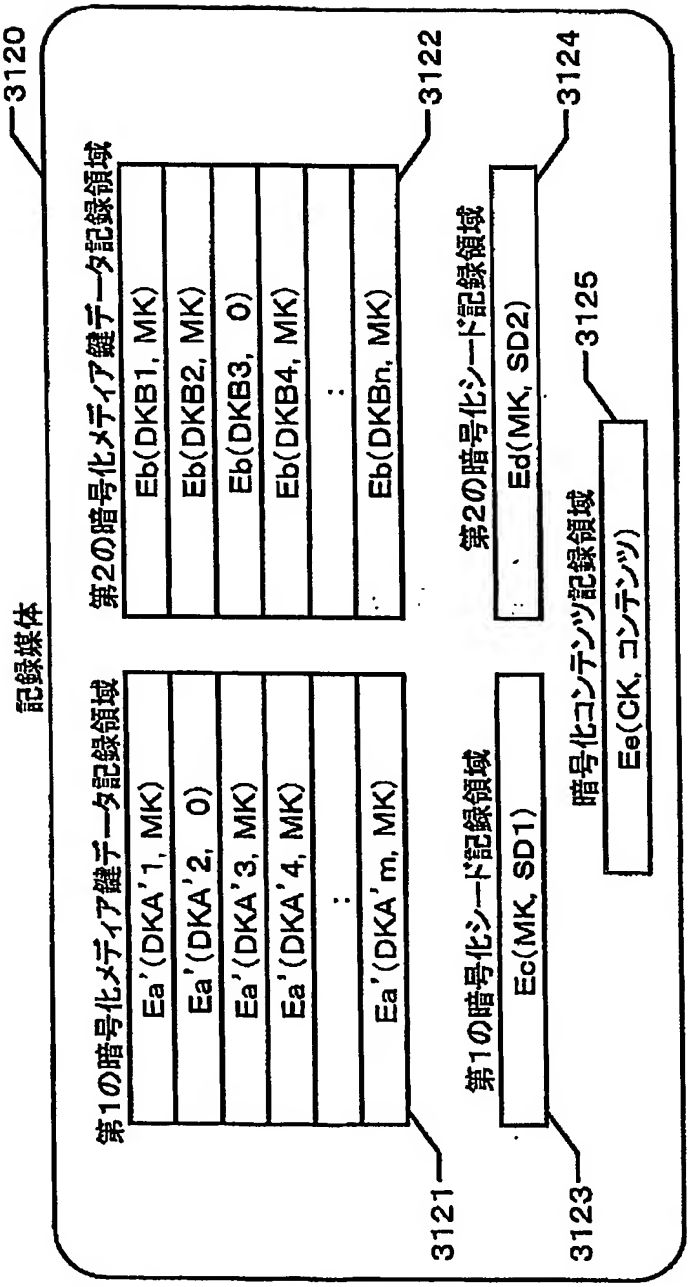

3120
記録媒体
第1の暗号化メディア鍵データ記録領域
Ea'(DKA'1, MK)
Ea'(DKA'2, 0)
Ea'(DKA'3, MK)
Ea'(DKA'4, MK)
Ea'(DKA'm, MK)
3121
第2の暗号化メディア鍵データ記録領域
Eb(DKB1, MK)
Eb(DKB2, MK)
Eb(DKB3, 0)
Eb(DKB4, MK)
Eb(DKBn, MK)
3122
第1の暗号化シード記録領域
Ec(MK, SD1)
3123
第2の暗号化シード記録領域
Ed(MK, SD2)
3124
暗号化コンテンツ記録領域
Ee(CK, コンテンツ)
3125

図37

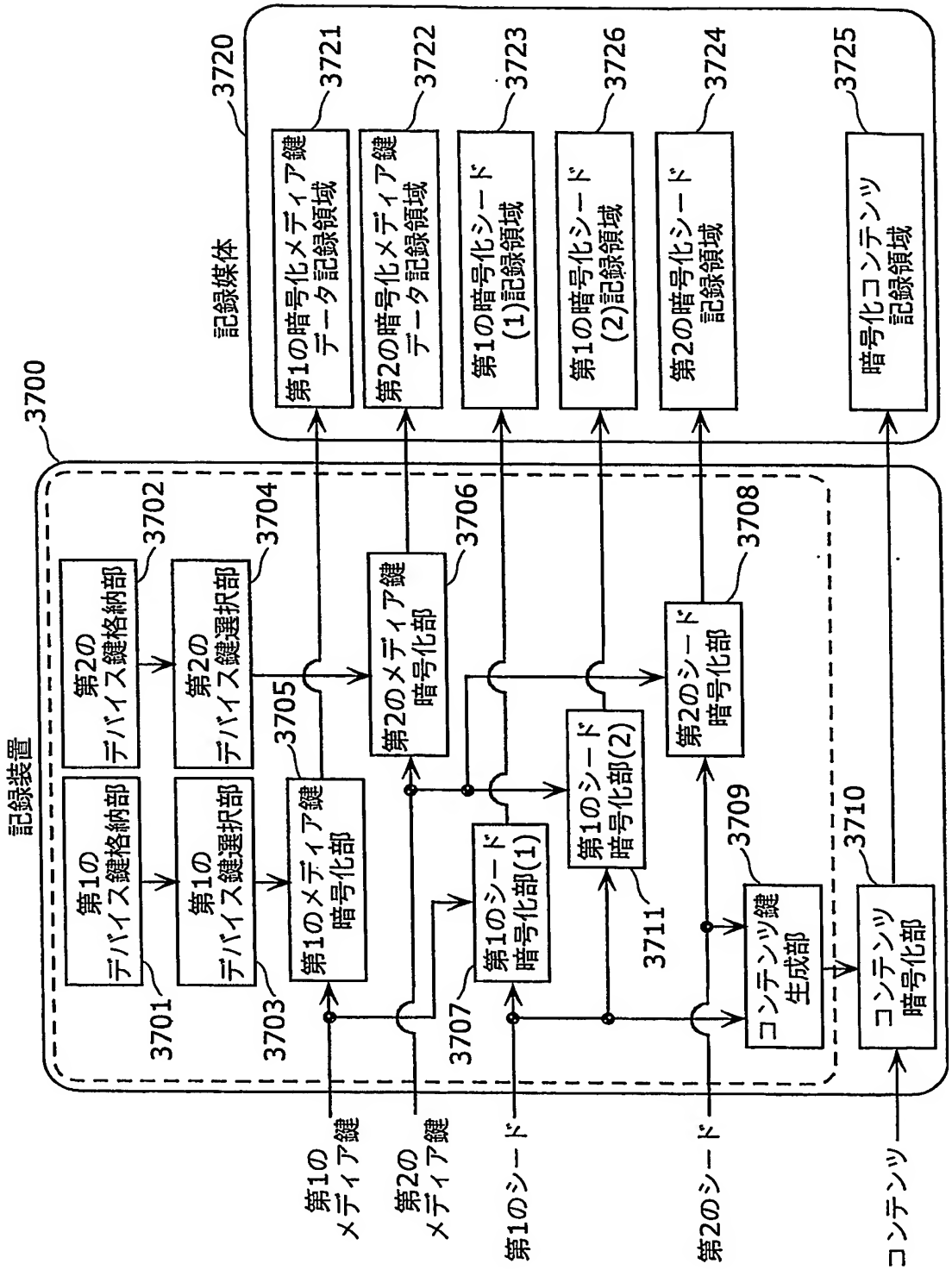

3700
記録装置
記録媒体
3720
第1の暗号化メディア鍵データ記録領域
3721
第2の暗号化メディア鍵データ記録領域
3722
第1の暗号化シード(1)記録領域
3723
第1の暗号化シード(2)記録領域
3726
第2の暗号化シード記録領域
3724
暗号化コンテンツ記録領域
3725
第1のデバイス鍵格納部
3701
第1のデバイス鍵選択部
3703
第2のデバイス鍵格納部
3702
第2のデバイス鍵選択部
3704
第1のメディア鍵暗号化部
3705
第2のメディア鍵暗号化部
3706
第1のシード暗号化部(1)
3707
第1のシード暗号化部(2)
3711
第2のシード暗号化部
3708
コンテンツ鍵生成部
3709
コンテンツ暗号化部
3710
第1のメディア鍵
第2のメディア鍵
第1のシード
第2のシード
コンテンツ

図38

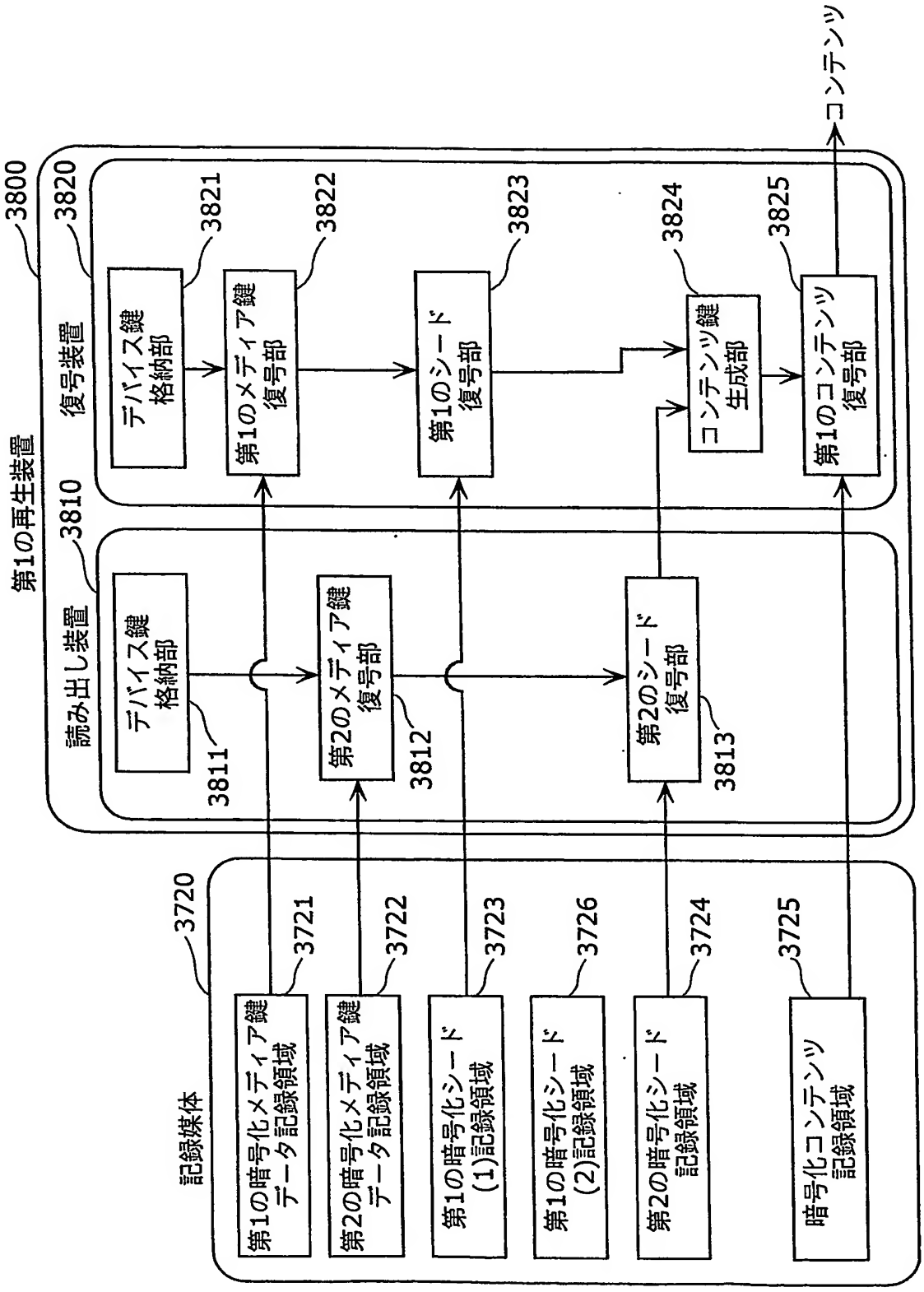

第1の再生装置
3800
読み出し装置
3810
復号装置
3820
デバイス鍵格納部
3811
第2のメディア鍵復号部
3812
第2のシード復号部
3813
デバイス鍵格納部
3821
第1のメディア鍵復号部
3822
第1のシード復号部
3823
コンテンツ鍵生成部
3824
第1のコンテンツ復号部
3825
コンテンツ
記録媒体
3720
第1の暗号化メディア鍵データ記録領域
3721
第2の暗号化メディア鍵データ記録領域
3722
第1の暗号化シード(1)記録領域
3723
第1の暗号化シード(2)記録領域
3726
第2の暗号化シード記録領域
3724
暗号化コンテンツ記録領域
3725

図39

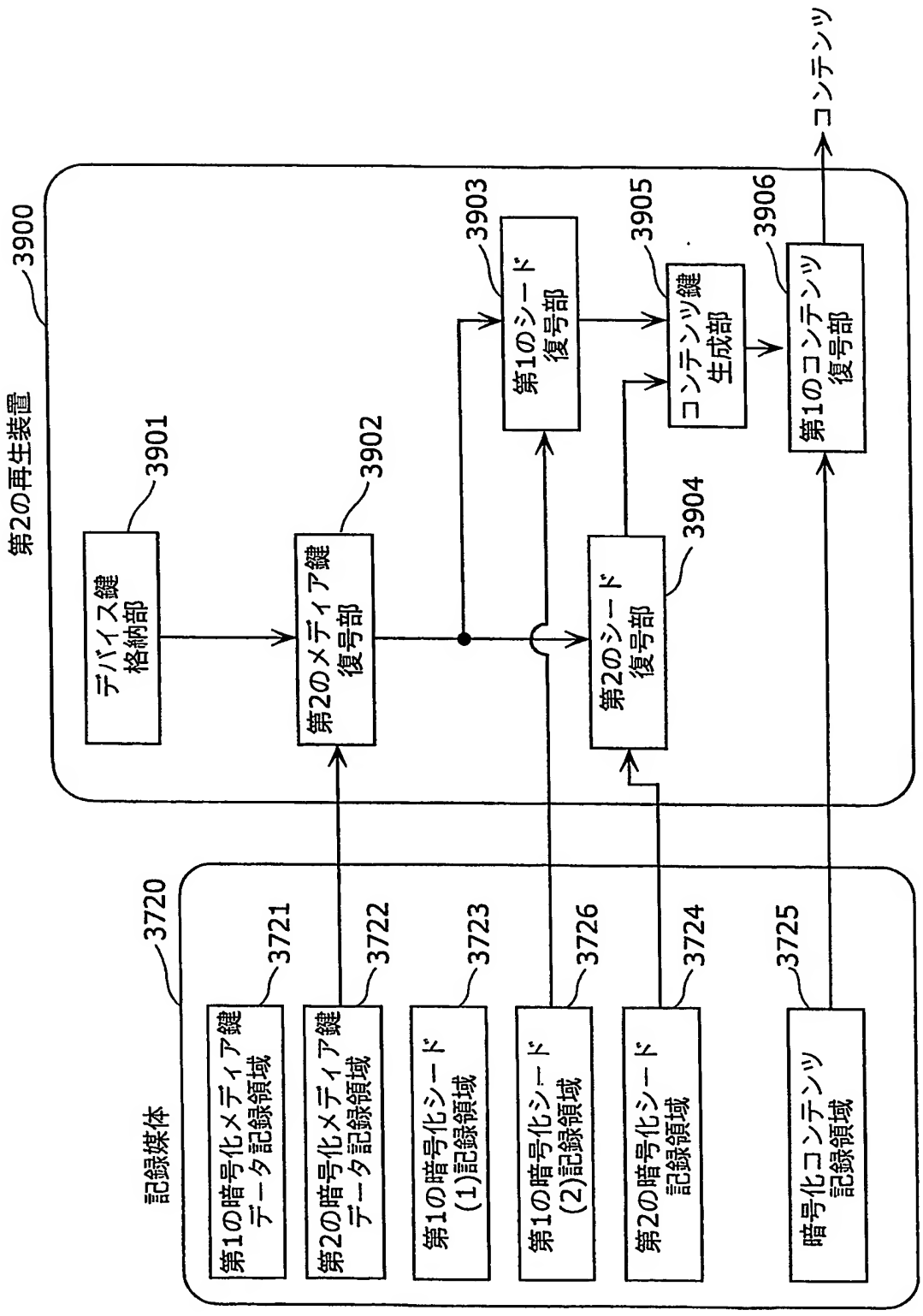

記録媒体
3720
第1の暗号化メディア鍵データ記録領域
3721
第2の暗号化メディア鍵データ記録領域
3722
第1の暗号化シード(1)記録領域
3723
第1の暗号化シード(2)記録領域
3726
第2の暗号化シード記録領域
3724
暗号化コンテンツ記録領域
3725
第2の再生装置
3900
デバイス鍵格納部
3901
第2のメディア鍵復号部
3902
第1のシード復号部
3903
第2のシード復号部
3904
コンテンツ鍵生成部
3905
第1のコンテンツ復号部
3906
コンテンツ

図40

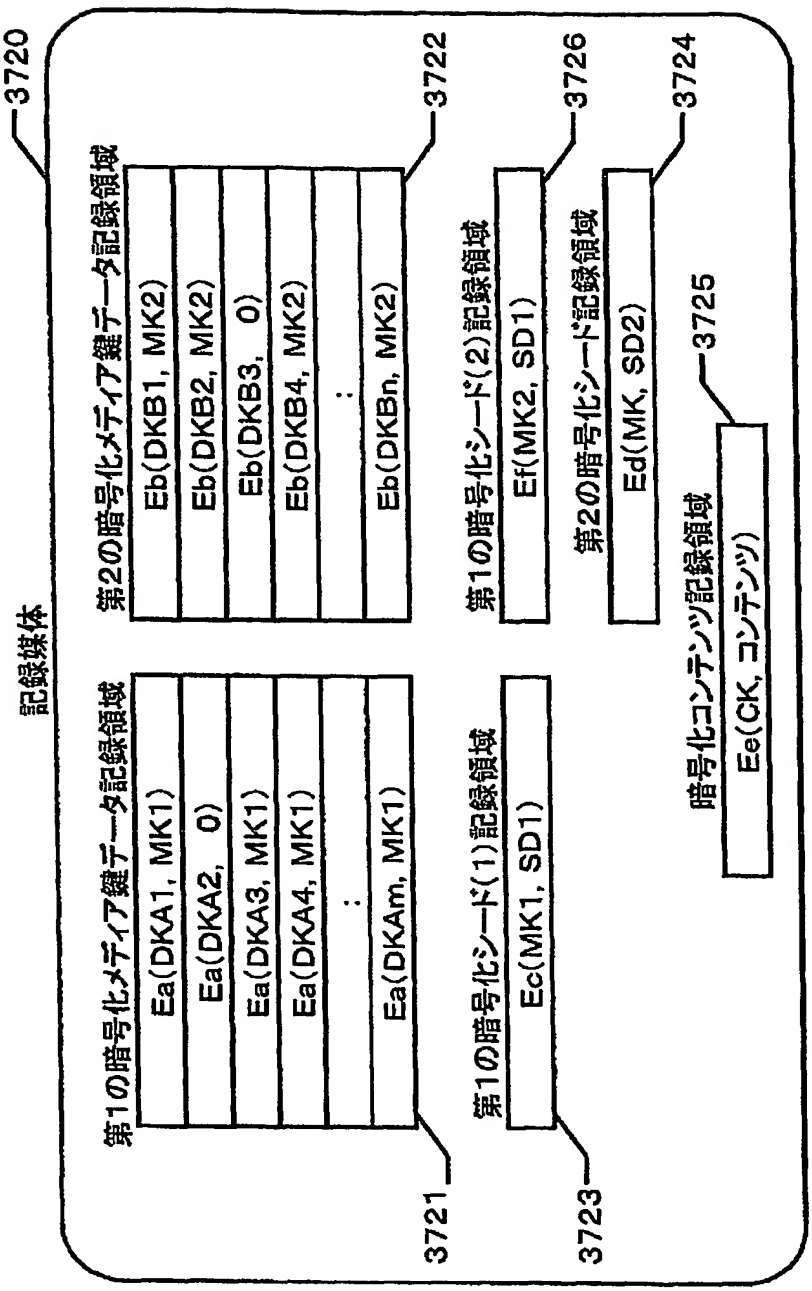

記録媒体
3720
第1の暗号化メディア鍵データ記録領域
Ea(DKA1, MK1)
Ea(DKA2, 0)
Ea(DKA3, MK1)
Ea(DKA4, MK1)
Ea(DKAm, MK1)
3721
第2の暗号化メディア鍵データ記録領域
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
3722
第1の暗号化シード(1)記録領域
Ec(MK1, SD1)
3723
暗号化コンテンツ記録領域
Ee(CK, コンテンツ)
3725
第1の暗号化シード(2)記録領域
Ef(MK2, SD1)
3726
第2の暗号化シード記録領域
Ed(MK, SD2)
3724

図41

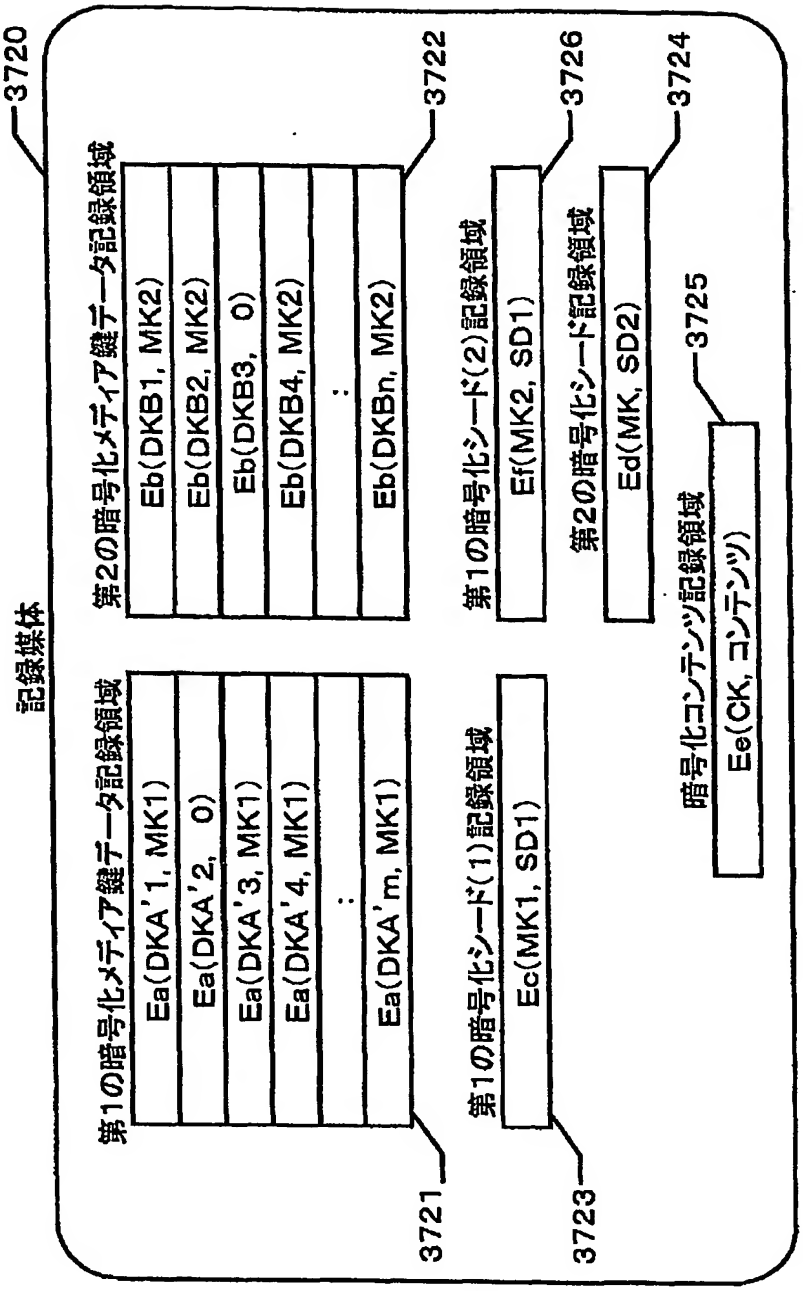
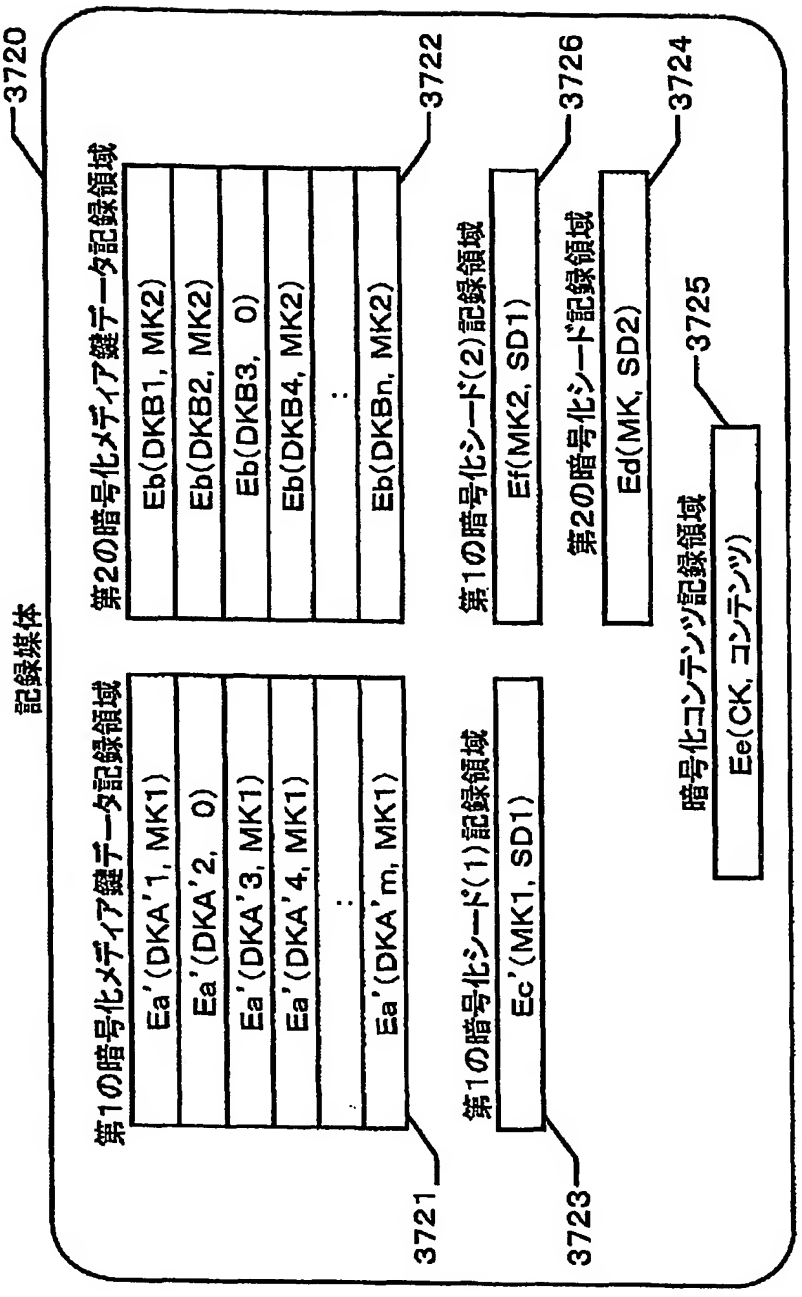

3720
記録媒体
第1の暗号化メディア鍵データ記録領域
Ea(DKA'1, MK1)
Ea(DKA'2, 0)
Ea(DKA'3, MK1)
Ea(DKA'4, MK1)
Ea(DKA'm, MK1)
3721
第2の暗号化メディア鍵データ記録領域
Eb(DKB1, MK2)
Eb(DKB2, MK2)
Eb(DKB3, 0)
Eb(DKB4, MK2)
Eb(DKBn, MK2)
3722
第1の暗号化シード(1)記録領域
Ec(MK1, SD1)
3723
第1の暗号化シード(2)記録領域
Ef(MK2, SD1)
3726
第2の暗号化シード記録領域
Ed(MK, SD2)
3724
暗号化コンテンツ記録領域
Ee(CK, コンテンツ)
3725

図42



差替え用紙(規則26)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011303

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Makoto Tatebayashi, Toshiharu HARADA, Yoshihisa FUKUSHIMA, Hideyuki ISHIHARA, "Kiroku Media no Contents Hogo System", 2000 Nen The Institute of Electronics, Information and Communication Engineers Kiso · Kyokai Society Taikai Koen Ronbunshu, 07 September, 2000 (07.09.00), pages 367 to 368	1-34
Y	JP 2000-23137 A (Matsushita Electric Industrial Co., Ltd.), 21 January, 2000 (21.01.00), Full text; Figs. 1 to 6 & TW 416246 B & EP 969667 A & CN 1249621 A & SG 71930 A & AU 741900 A & US 6714649 B	1-34

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 26 October, 2004 (26.10.04)	Date of mailing of the international search report 16 November, 2004 (16.11.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011303

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-181689 A (Sony Corp.), 12 July, 1996 (12.07.96), Par. Nos. [0025], [0028] to [0033], [0054] to [0067]; Figs. 1, 2, 7 & EP 710025 A & US 5721778 A & EP 996288 A & JP 2000-316144 A & JP 2003-46497 A & JP 2003-264550 A	6,25-27

国際調査報告

国際出願番号　PCT／JP2004／011303

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　　H04L9／08

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　　H04L9／08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	館林誠，原田俊治，福島能久，石原秀志，“記録メディアのコンテンツ保護システム”，２０００年電子情報通信学会基礎・境界ソサイエティ大会講演論文集，２０００．０９．０７，ｐ．３６７－３６８	１－３４
Y	ＪＰ　２０００－２３１３７　Ａ（松下電器産業株式会社）　２０００．０１．２１　全文，図１－６　＆　ＴＷ　４１６２４６　Ｂ　＆　ＥＰ　９６９６６７　Ａ　＆　ＣＮ　１２４９６２１　Ａ　＆　ＳＧ　７１９３０　Ａ　＆　ＡＵ　７４１９００　Ａ　＆　ＵＳ　６７１４６４９　Ｂ	１－３４

☒ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　26．10．2004	国際調査報告の発送日　16.11.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　5M　4229 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５９７

様式PCT／ISA／210（第2ページ）（2004年1月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　８－１８１６８９　Ａ（ソニー株式会社） １９９６．０７．１２ 第【００２５】段落，第【００２８】－【００３３】段落， 第【００５４】－【００６７】段落，図１，２，７ ＆　ＥＰ　７１００２５　Ａ　＆　ＵＳ　５７２１７７８　Ａ ＆　ＥＰ　９９６２８８　Ａ ＆　ＪＰ　２０００－３１６１４４　Ａ ＆　ＪＰ　２００３－４６４９７　Ａ ＆　ＪＰ　２００３－２６４５５０　Ａ	6, 25-27